Acano solution

Security Considerations

August 2015

76-1026-01-E

Contents

1 Introduction

This document is an outline of the ways in which the Acano solution is designed, coded and implemented with security in mind.

2 Acano Secure Development Lifecycle

The Acano Secure Development Lifecycle is the methodology we employ to ensure that security is considered at each step of the software development process. The lifecycle has seven phases – as described in this section.

At Acano we recognize that management buy-in isn't enough to ensure that security is a focus: you need boots on the ground. At Acano, our Security Advocates are a virtual community of knowledgeable, security-minded individuals selected from each development group to evangelize security right at the point where software is created.

In summary, Acano has a high level vision for secure software development backed by committed developers who make sure that these values translate into actions.

1. **Training**: We train our software developers, testers and managers in the core security concepts required to build better, more secure software. This includes concepts in secure design, secure coding practices, threat modeling and penetration testing.
2. **Requirements**: At Acano, we draw our requirements for security from the most stringent of government and industry standards (FIPS, JITC etc.), from feedback from partners and from analysis of emerging threats. The security requirements for all Acano products are codified in our Security Baseline.
3. **Design**: From the complete solution level down to individual components, we analyze designs from the perspective of an attacker. We consider the attack surface and model threats to make sure that mitigations are part of the design.
4. **Implementation**: At Acano, we follow the secure coding standards developed by CERT (https://www.securecoding.cert.org). We use static analysis tools and targeted code reviews to reduce software defects in general but prioritize possible security issues.
5. **Verification**: The system is verified by automated fuzz and stress testing, alongside penetration testing. At this point, the attack surface is reconsidered to make sure that it is the same as envisaged at the design stage and that the each mitigation has been implemented.
6. **Release**: For each release, there is an Incident Response Plan. The plan designates a rota of Acano employees who can be contacted 24 hours a day, 365 days a year and who are empowered to take actions to address threats which emerge over time.
7. **Response**: In the event that a security vulnerability is discovered, Acano will notify customers in a timely fashion to explain the extent of the problem, mitigations that can be employed and, if necessary, to give a timeline for the release of updated software to address the issue.

3 Acano Security Points

General design features for security are:

- Password-protection for access to the MMP interface and Web Admin Interface

  Industry-standard password management rules to enforce secure password usage (see MMP command line interface guide section 6.1)

  The MMP commands configure the Acano Core and Edge software.

  It is up to users to ensure the physical security of the Acano Servers or the server(s) that the virtual deployment runs on. There are no default credentials on the system and physical access is required to perform a credential reset using a protected Reset button. Equally, there are no Acano-facing backdoors; that is, there are no secret passwords or keys which Acano retains.

  Password hashing conforms to the US Federal standard. Administration passwords are configurable for length, complexity, reuse and age to enable compliance with strict password guidelines.

  The Web Admin Interface exposes status information and the ability to download logs as well as the pages to configure the Call Bridge.
- The Acano Server is configurable even when under denial of service attack: the MMP is an out-of-band configuration interface
- Domain Name System Security Extensions (DNSSEC)

  DNS has many weaknesses: several of these trust issues are addressed by DNSSEC. As the rollout of DNSSEC gathers pace, Acano is ready to use it with only minor configuration steps.

  We also address some of the inherent weaknesses of DNS by making DNS spoofing difficult (for example by choosing source ports for DNS queries randomly and by strictly parsing responses), and by allowing the configuration of failover recursive servers.

  Acano offers fine grained control over which recursive servers should be queried by allowing the configuration of forwardzones. This offers a secure method to provide multiple domains in a multi-tenant setup.
- Field industry-standard strong cryptography protection of communications

  We use FIPS-140-2 level 1 approved (or better) cryptography throughout the Acano solution. We implement all our cryptography in the same OpenSSL codebase which is advantageous for secure management of the code, and is uncommon in the industry where inhomogenous processing is used i.e. they use DSPs with custom cryptography stacks. (A large and active developer and user base for OpenSSL is good for the security of our product.) By default, we use TLS to protect signaling and SRTP to protect media. Web services default to using HTTPS with configurable redirect from HTTP (nothing else is carried by HTTP). There are no plaintext configuration protocols in use such as telnet and FTP, we use SSH and SFTP instead.
- API access that is only available via TLS
- The destination for Call Detail Records can be configured as an "HTTPS" address to enforce TLS encryption for this information

- Detailed audit logs are stored on disk with capability to forward by syslog to multiple syslog servers for external storage
- The Acano Server has dual power, multiple compute modules and redundant fans to keep services going under hardware failures.
- The software architecture is compartmentalized to prevent a software failure causing long outages
- Backup and restore functionality of complete configuration including coSpace data for continuity of service and rapid hardware swapout
- Firewall deployment

  It is possible to deploy the Acano solution entirely behind the firewall, publishing only specific ports required for external access. On the Acano Server there is no physical separation between the media interfaces A-D but the MMP interface is physically separate being accessed on the Admin interface. Each interface is configured independently of the others at the IP level. IP forwarding is not enabled in either the MMP or host IP stack.
- SHA-1 and SHA-2 signed certificates

  The Acano solution supports certificates signed using SHA1 and SHA2 algorithms. When the Acano server creates certificate signing requests, they are signed using SHA256 in accordance with rules which CAs now operate under.

Data protection

- IP media (video and audio) is AES encrypted (industry-standard SRTP)

  The Advanced Encryption Standard is used worldwide for the encryption of electronic data and is used by the US government to encrypt secret documents. It superseded previous standards. More specifically Acano supports AES-CM 128 bit and 256 bit ciphers with SHA1-80 or SHA1-32 authentication.

  We conform to the specification of AES as presented in ISO/IEC 18033-3, but our efforts at validation are towards FIPS. We have FIPS 140-2 Level 1 validation for our cryptography code. It's 1747 on this link http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm, we are listed as AcanOS (our Linux based operating system).
- All control data can be authenticated/encrypted (industry-standard TLS/SSL)

  TLS connections require certificate authentication. This is used between the Acano solution and external devices (such as a Lync server), and is also used internally. Acano uses OpenSSL an open-source implementation of TLS and SSL
- All data on the box is encrypted at rest using 256-bit AES encryption

  To destroy data on the disk we destroy the encryption keys. This is a secure and disk friendly way to erase data. Recovery of the data should be computationally impossible but is theoretically possible if the disk is analyzed forensically outside of the box. This will be removed using Clean Slate erasure.

Client and in-call features

- User login password protection
- coSpaces can have a security code/pin

  Each coSpace can have a security pass code set, which prevents people who do not know this pass code from connecting to the coSpace.

- On-screen visual indication of audio-only participants

  When there are participants in the call that can hear and see media from the other participants, but cannot be seen themselves, they contribute towards an on-screen counter of the number of audio-only participants present.

- On-screen indication of “encrypted” participants

  - SIP endpoints use their normal encryption indicators to indicate that their call leg is encrypted. Acano clients always encrypt media and also display an indicator in the Call info pane in the Call view.
  - The Acano clients will encrypt by default (as the only mode of operation). However, for SIP endpoints the Acano solution supports media encryption for SIP connections including Lync calls. This feature is not enabled by default in case it causes interoperability issues with some devices. Note that enabling encryption only affects new calls, not those calls already in progress, and that the settings’ value will persist over a restart.