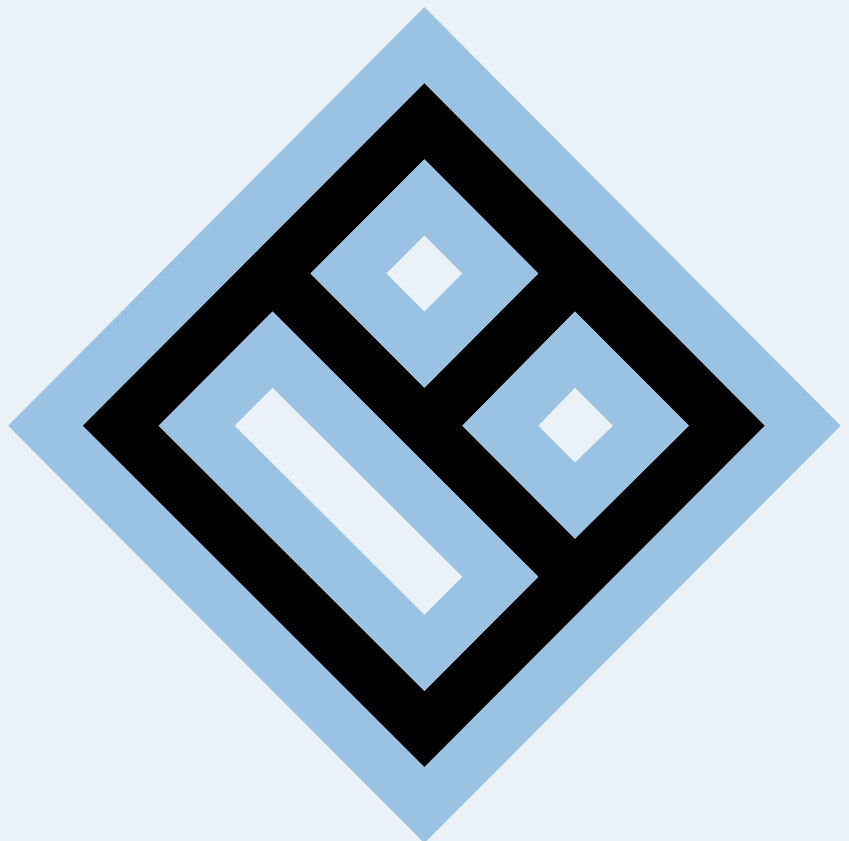




NEXTRAGEN

NEXT GENERATION TESTING

TraceSim 3.0: Erweiterte Messung im Bereich Secure-VoIP und erstmals Simulation von Video im Netzwerk



Kein Teil dieser Broschüre darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder in einem anderen Verfahren) ohne unsere vorherige schriftliche Genehmigung reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Wir weisen darauf hin, dass die im Dokument verwendeten Bezeichnungen und Markennamen der jeweiligen Firmen im Allgemeinen Warenzeichen, marken- oder patentrechtlichem Schutz unterliegen.

Copyright: 2012 Nextragen GmbH
Stand: 01/2012

Herausgeber:
Nextragen GmbH
Lise-Meitner-Str.2
24941 Flensburg

Germany

Management Summary

Das von Nextragen entwickelte Mess- und Analysekonzept TraceSim stellt, in der Version 3.0, jetzt auch die in der Voice over IP-Welt notwendigen Sicherheitsfunktionen zur Verfügung. Gleichzeitig wird mit diesem Release erstmals die Videotechnik (Video conferencing, Videostreaming) unterstützt. Damit bietet TraceSim VoIP 3.0 dem Netzadministrator ein noch umfassenderes Werkzeug zur aktiven Netzwerküberprüfung, das durch die Generierung von VoIP/Video-Gesprächen alle relevanten VoIP-, Video- und QoS-Parameter ermittelt und detailliert darstellt. Besonderes Augenmerk legt die neue Version von TraceSim auf eine Senkung von Zeit- und Kostenaufwand im Umfeld des VoIP-Betriebs und trägt somit entscheidend zur Erhöhung der Wirtschaftlichkeit und zur Verbesserung der Produktivität bei.

Inhaltsverzeichnis

Management Summary.....	3
Inhaltsverzeichnis	4
Die Neuerungen von TraceSim 3.0 auf einen Blick.....	5
VoIP-Sicherheit und Video over IP erfordern die richtige Messtechnik	5
Sicherheit in Netzen steht an oberster Stelle	5
Secure Real-Time Transport Protocol	6
Transport Layer Security (TLS).....	7
TraceSim 3.0 unterstützt jetzt auch SRTP und TLS.....	7

Die Neuerungen von TraceSim 3.0 auf einen Blick

Das Softwaretool TraceSim VoIP zur aktiven Simulation von VoIP- und Video-Verbindungen wurde in der neuen Version 3.0 für das Marktsegment der VoIP/Video-Analyse um zahlreiche Zusatzfunktionen erweitert. Zu den neuen Funktionen von TraceSim 3.0 gehören:

TLS/SRTP

- SRTP gemäß RFC: 3711
 - AES_CM_128_HMAC_SHA1_80
 - AES_CM_128_HMAC_SHA1_32
 - SRTCP
 - SDESC gemäß RFC 4568
- TLS
 - SIP over TCP / TLS

Video

- Simulation von Video-Calls (beispielsweise gegen ein anderes TraceSim oder Test Agenten)
- stufenlose Bandbreitenauswahl
- Video- und Audio-Channel separat schaltbar
- Berechnung von MOS nach PEVQ
- Unterstützung der Codecs H.263 und H.264
- mehrere parallele Video-Streams gleichzeitig
- Betrachtung des gesendeten und empfangenen Streams

VoIP-Sicherheit und Video over IP erfordern die richtige Messtechnik

Die Anforderungen an die Unternehmensnetze wachsen durch den Einsatz von VoIP und Video drastisch an und die Ende-zu-Ende Qualität wird zum entscheidenden Erfolgsfaktor für alle Echtzeitapplikationen. Aus diesem Grund müssen sich die Administratoren rechtzeitig mit den richtigen Messwerkzeugen zur Fehlersuche und zur Analyse auseinandersetzen, um bei Problemen die Ursachen schnell und kostengünstig feststellen zu können.

Zur CeBIT 2012 veröffentlicht die Nextragen GmbH das neue TraceSim Version 3.0. Dieses erweitert die Mess-, Simulations- und Analysefunktionen um die Bereiche VoIP-Sicherheit und Video over IP. Das Messwerkzeug orientiert sich an der bewährten Analysetechnik und bietet dem Anwender praxisnahe Messeigenschaften. Dadurch sind mögliche Fehler im VoIP- und/oder Video-Netzwerk noch genauer zu ermitteln und auf Basis einer einzigen Messung kann eine zielgenaue Aussage über die Ursache im Netzwerk getroffen werden.

Sicherheit in Netzen steht an oberster Stelle

Immer mehr Firmen wird bei einem Ausfall der IT bewusst, wie stark sich dieser auf den Unternehmenserfolg auswirken kann. Daher zählt die IT-Security heute zu den wichtigsten Grundpfeilern jedes Unternehmens. Durch die Netzwerkkonvergenz wird dieser Effekt noch weiter verschärft. Konnte man bisher bei einem Versagen des Internets noch das Telefonnetz benutzen und so z.B. den Ausfall der E-Mail-

Kommunikation durch das Fax kompensieren, wird es in Zukunft diese Möglichkeit nicht mehr geben.

Während bei der traditionellen Telefonie spezielle Hard- und Software zum Ausspionieren und Manipulieren der Datenübertragung nötig ist, ist es einem Angreifer bei VoIP möglich, auf normale und weit verbreitete Hacker-Werkzeuge zu setzen. Ist beispielsweise bei ISDN ein spezieller Hardware-Analysator notwendig, um den Datenstrom aufzuzeichnen und zu analysieren, liefert bei SIP und RTP eine Freeware die gleiche Funktionalität. Dadurch verringert sich der Aufwand, den ein potentieller Angreifer überwinden muss, um ein VoIP-System anzugreifen.

Daher gilt es folgende Sicherheitsziele im VoIP-Netz zu etablieren:

- Vertraulichkeit: Darunter versteht man, dass sensible Daten vor dem Zugriff unberechtigter Dritter geschützt werden. Bei VoIP sind vor allem die Vertraulichkeit der Gespräche und der Verbindungsdaten wichtig.
- Integrität: Die Integrität der benutzten Daten und Geräte muss sichergestellt werden, um beide vor einer Manipulation durch Dritte zu schützen. Bei VoIP ist dabei die Integrität der Signalisierungsdaten, der Netzwerkgeräte (Software, Konfigurationsdateien) und der Verbindungsdaten wichtig.
- Verfügbarkeit: Besonders bei kritischen Anwendungen (z.B. einem Anruf bei einer Notrufzentrale) ist oftmals eine hohe Verfügbarkeit, auch unter widrigen Umständen, erforderlich. Dabei ist es nicht nur wichtig, dass die Applikation im Normalbetrieb oder bei Belastungsspitzen läuft, sondern auch bei Angriffen ihren Dienst verrichtet.
- Verbindlichkeit: Unter Verbindlichkeit versteht man, dass über IP Telefonie getätigte Transaktionen rechtskräftig sind.
- Authentifizierung: Authentifizierung ist die Überprüfung, ob eine Person wirklich die ist, die sie vorgibt zu sein.

- Zugriffskontrolle /Autorisation: Hierbei geht es darum, welche Rechte einem User zugeordnet werden. Entscheidend ist hierbei die Granularität der Rechtevergabe, sprich, wie genau können wem welche Rechte zugewiesen werden.

Es gibt zahlreiche Angriffe, gegen die ein VoIP-System geschützt werden muss. Eine einzige Sicherheitslücke reicht aus, um das ganze VoIP-System zu gefährden.

Secure Real-Time Transport Protocol

Das Ziel des Secure Real-Time Transport Protocols (SRTP) besteht darin, RTP und RTCP so zu erweitern, dass die Vertraulichkeit der Kontroll- und Nutzdaten gegenüber Dritten gesichert sind. Ein weiteres Feature von SRTP ist die leichte Integration in bestehende RTP/RTCP-Protokollstacks, weil es die bestehende Headerstruktur nur um einige neue Felder erweitert. SRTP wurde von der IETF im RFC 3711 dokumentiert.

SRTP regelt nur, wie aus einem bestehenden Masterkey die, für die Authentifizierung und Verschlüsselung verwendeten Sessionschlüssel bzw. der Salt berechnet wird. Wie der Masterkey zwischen den Geräten verteilt wird, lässt die Spezifikation (noch) offen.

Wie bereits oben erwähnt, schreibt SRTP die Verschlüsselung von Nutz- und Kontrolldaten zwingend vor. Zur Verschlüsselung sieht der RFC 3711 einen 128 Bit langen AES Algorithmus vor. Um die Daten vor Verfälschungen zu schützen, werden die verschlüsselten Daten mit einem 128 Bit HMAC-SHA-1 Algorithmus und dem speziel-

len Authentifizierungsschlüssel gehasht. Als Schutz vor Replay Attacks ist ein Index mit den bereits empfangenen Paketen vorgeschrieben. Pakete, die gemäß dieser Liste bereits einmal empfangen wurden, werden ignoriert.

Transport Layer Security (TLS)

Die Transport Layer Security TLS ist ein im RFC 2246 spezifiziertes Protokoll, das auf dem Secure Sockets Layer (SSL) Version 3.1 basiert und einen sicheren, d.h. authentischen und vertraulichen Kanal auf der Transportschicht implementiert. Die SIP Spezifikation RFC 3261 schreibt vor, dass alle konformen SIP Server (Proxy-Server, Redirect-Server, Location-Server und Registrar-Server) das TLS Protokoll mit gegenseitiger Authentifizierung sowie Einweg-Authentifizierung unterstützen müssen. Des Weiteren sollte zumindest die Cipher-Suite TLS_RSA_WITH_AES_128_CBC_SHA von allen TLS unterstützenden SIP Anwendungen implementiert werden.

Durch die Verwendung eines SIPS Request-URI wird die Verwendung von TLS mit gegenseitiger Authentifizierung und TLS_RSA_WITH_AES_128_CBC_SHA Cipher-Suite angefordert. Der SIP Standard fordert, dass konforme Implementierungen dieser Aufforderung nachkommen sollten. UAs sollten TLS verwenden, um ihre Kommunikation mit Proxy-, Redirect- sowie Registrar-Servern zu schützen.

Die Verwendung eines SIPS URI bedeutet, dass jeder Hop bis zur Ziel-Domain durch die Verwendung von TLS geschützt werden sollte. Der letzte Hop vom Proxy der Zieldomain zum UA muss ebenfalls gesichert werden, wobei der dabei eingesetzte Sicherheitsmechanismus durch die Sicherheitspolitik innerhalb der Ziel-Domain bestimmt wird.

TLS 1.0 gilt als sicheres, etabliertes Protokoll mit vielen, teilweise frei verfügbaren Implementierungen, was eine schnelle Verbreitung auf dem VoIP-Markt verspricht. Da es auf Zertifikaten basiert, kann es zwischen Systemen zum Einsatz kommen, die zuvor keine Vertrauensbeziehung (beispielsweise in Form gemeinsamer symmetrischer Schlüssel) besitzen besaßen.

TLS bietet im Kontext von SIP Systemen nur Hop-to-Hop Sicherheit zwischen je zwei benachbarten Hops. Dies hat auf der einen Seite Vorteile, weil einzelne Hops ohnehin Zugriff auf Teile der Klartextnachrichten haben müssen, beispielsweise, um diese an die richtigen Domains weiterleiten zu können. Auf der anderen Seite muss man sich aber auch der Tatsache bewusst sein, dass dadurch keine echte Ende-zu-Ende Sicherheit erreicht werden kann. Hier müssen die Endgeräte allen Proxy-Servern entlang des Signalisierungspfades vertrauen.

TLS setzt eine zuverlässige Transportschicht voraus. Somit können durch SIPS initiierte TLS-geschützte Sessions nicht über UDP initiiert werden, was den Overhead durch TCP-basierte Signalisierung erhöht.

TraceSim 3.0 unterstützt jetzt auch SRTP und TLS

Das Softwaretool TraceSim zur aktiven Simulation von VoIP-Verbindungen wurde in der neuen Version 3.0 um die Unterstützung der SRTP-Funktionen (gemäß RFC: 3711 und die Transport Level Security (TLS) erweitert.

Das Nextragen-Produkt unterstützt im Bereich SRTP die gängigen AES-Varianten HMAC_SHA1_80 und HMAC_SHA1_32. Auch die RTP-Kontrollsequenzen werden in

der Version 3.0 gesichert (gemäß SRTCP) zwischen den Kommunikationspartnern ausgetauscht. Darüber hinaus sorgt die neueste TraceSim-Variante für den gesicherten Schlüsselaustausch nach RFC 4568.

Durch die vollständige Implementation der Transport Level Security (TLS) ist TraceSim in der Lage, die SIP-Informationen über eine gesicherte Transportverbindung (SIP over TCP/TLS) zu übermitteln.

TraceSim 3.0 bietet durch die Sicherheitserweiterungen im Bereich VoIP dem Administrator und Techniker ein einfach zu bedienendes Werkzeug zur aktiven Netzwerküberprüfung auch im Umfeld der erhöhten Sicherheitsanforderungen für VoIP. Durch die Verschlüsselung der Signalisierung und der VoIP-Nutzlasten bei der Generierung von VoIP-Gesprächen werden alle relevanten VoIP- und QoS-Parameter ermittelt und detailliert dargestellt. Die integrierten Messalgorithmen überprüfen die aktuelle Sprachqualität und dokumentieren diese auf einer Ende-zu-Ende-Basis. Auf bis zu 300 parallelen Verbindungen werden dabei echte VoIP-Lasten übertragen und die aktuellen Priorisierungsmechanismen über ein Netzwerk oder einer WAN-Strecke hinweg bis in die Details getestet.

Weitere Baustellen im Netzwerk: Videoübertragung und interaktive Videokonferenzen

Die Einführung von Voice over IP ist jedoch nur die Spitze des Eisbergs. Daher ist es nicht verwunderlich, dass die Videoübermittlung und das Videoconferencing mit Vehemenz in die Netzwerke einbrechen. Nachteilig an diesen Applikationen ist jedoch, dass diese eine hohe Bandbreite benötigen und außerdem sehr empfindlich auf Störungen im Netzwerk reagieren. Ohne das richtige Know-how und die entsprechenden Messinstrumente steht der Administrator vor einem fast unlösbaren Problem.

Das Videoconferencing stellt gegenüber der reinen Übermittlung von Bewegtbildern (Überwachungskameras) eine eigenständige Kommunikationssituation dar, die nicht bloß auf der Mitte zwischen traditioneller Telefon- und Face-to-Face-Kommunikation liegt. Das wichtigste Problem ist dabei, dass aus den räumlich getrennten Standorten der Teilnehmer unterschiedliche Wahrnehmungsbedingungen resultieren. Bei einer Videokonferenz werden die gesammelten isochronen Bild- und Toninformationen über das Netz übermittelt. Bezeichnend für das Videoconferencing ist, dass zwischen den Teilnehmern immer eine Punkt-zu-Punkt- bzw. Punkt-zu-Mehrpunkt-Kommunikationsbeziehung entsteht. Aus diesem Grund scheidet das bei der klassischen Videoübermittlung von Filmen zur Bandbreiteneinsparung genutzte Multicasting aus. Die bidirektionalen Videoinformationen werden von der IP-Plattform in Real Time Protocol (RTP)-Pakete verpackt und auf die Reise geschickt. Das für die Kommunikation von Echtzeitanwendungen konzipierte RTP nutzt für den Datentransport das UDP-Protokoll (User Datagram Protocol). UDP ist ein verbindungsloser Datenübertragungsdienst, der keinerlei Kontroll- und Steuermechanismen für das Verbindungsmanagement bereitstellt. Für die fehlenden Mechanismen sorgt das RTP.

Im Datenteil des RTP-Pakets befinden sich die eigentlichen Rohdaten. Die Informationen wurden vom Sender in Abhängigkeit vom jeweiligen Codec codiert. Bei einem Codec handelt es sich um einen Algorithmus, der dafür sorgt, dass die zu übertragenden Bild- und Tondaten in digitale Informationen gewandelt werden. Der Codec ist ausschlaggebend für die Qualität der Übertragung. Bestimmte Codecs versenden die Ton- und Bilddaten direkt und verzichten auf eine Kompression. Andere Codecs nutzen unterschiedliche Komprimierungsverfahren, um die zu übermittelnde Datenmenge so gering wie möglich zu halten. Die hieraus resultierende Verkleinerung der

zu übermittelnden Datenmenge resultiert in einer Verschlechterung der Bild/Signalqualität. Die folgenden Codecs werden heute am häufigsten genutzt: H.263 und H.264.

Durch gezielte Messungen lassen sich die im Datenpfad auftretenden Fehler analysieren und mit Hilfe der Mess-Software die Fehlerursachen ermitteln. So können beispielsweise mit einem auf Videoconferencing bzw. die unidirektionale Übermittlung von Videos spezialisierten Analysator die applikationsspezifischen Qualitätsparameter und Timing-Werte ermittelt und analysiert werden. Die vom Netzwerkanalysator zur Verfügung gestellten Parameter werden anschließend in den jeweiligen Berechnungsmodellen verarbeitet und liefern eine Art Video-MOS-Wert, mit dem sich die Güte einer Videoverbindung beurteilen lässt. Der MOS-Wert ist ein Wert ähnlich den Schulnoten zwischen eins und fünf. Dabei steht der Wert »1« für eine mangelhafte Sprachqualität, bei der keine Verständigung möglich ist, der Wert »5« hingegen signalisiert eine exzellente Übertragungsqualität, die nicht von dem Original zu unterscheiden ist.

TraceSim wurde speziell für das richtige Messen innerhalb von Videosystemen entwickelt und verfügt über zahlreiche Zusatzfunktionen, wie Verbindungslisten, Erfassung von Qualitätsmerkmalen usw.. Mit Hilfe der Simulation lassen sich detaillierte Aussagen über die zu erwartende Qualität der Videoübertragung treffen. Die integrierte PEVQ (Perceptual Evaluation of Video Quality) Messung basiert auf der von der ITU (International Telecommunication Union) verabschiedeten Spezifikation ITU J.247 und dient der aktiven Bewertung der Videoqualität bei der Übermittlung über Netzwerke. Dabei wird ein definiertes Referenzsignal über das Netzwerk zum betreffenden Kommunikationspartner übertragen und auf der Gegenseite aufgezeichnet. Anschließend wird das aufgezeichnete Signal mit dem Referenzsignal verglichen. Der PEVQ-Algorithmus bestimmt anhand dieser Daten die spezifische Qualität der Ende-zu-Ende-Übertragungstrecke. Mithilfe des in die Nextragen-Produkte integrierten Job-Planers lassen sich die Messabläufe auch automatisieren, um eine ständige Überwachung und Kontrolle des Netzwerkes zu gewährleisten. Ein umfangreiches Reportingtool sorgt für die notwendige Dokumentation der Messergebnisse. Bei der Darstellung der Protokolldaten wurde auf Übersichtlichkeit und leichte Bedienbarkeit geachtet, so dass der Anwender schnell den Umgang mit den Messwerkzeugen erlernt.

Bisher stellte TraceSim nur die notwendigen Mechanismen zur Messung, Simulation und Analyse von VoIP-Datenströmen zur Verfügung. Durch Ausbreitung der Video- und Videokonferenzsysteme werden zunehmend auch kombinierte Audio-/Videosignale über typische IP-Netze zu übertragen. Video over IP konkurriert dabei um die gleichen Rechner- und Übertragungsressourcen wie beispielsweise Voice over IP (VoIP). Mit TraceSim 3.0 lassen sich jetzt auch die Netzwerke auf ihre „Video Readiness“ überprüfen.



Firmenprofil Nextragen

Die Nextragen GmbH ist auf die Entwicklung von VoIP-/Video-Produkten und Software-Lösungen rund um die Themen "Testing, Monitoring und Analysing" ausgerichtet. Die Sicherstellung der End2End Dienste-Qualität (QoS, QoE) für Next Generation Networks und Triple Play Dienste steht im Fokus des Unternehmens. Nextragen-Messlösungen helfen unseren Kunden aus den Bereichen Carrier, Enterprise, Systemintegratoren und IT-Dienstleistern Investitionen in Netzwerkinfrastruktur und Triple - Play-Dienste wie Voice-over-IP, Video und IPTV zu sichern, operative Kosten zu reduzieren und den Anwendern durchgängig hochwertige Dienstqualität zur Verfügung zu stellen. Weitere Informationen erhalten Sie auf der Firmenwebsite unter www.nextragen.de.

Nextragen GmbH
Lise-Meitner-Str.2
24941 Flensburg
Germany

Telefon: +49 461 9041-4440
Fax: +49 461 9041-4449

www.nextragen.de
info@nextragen.de

Änderungen und Irrtümer vorbehalten