envoy Whitepaper

Warum ist envoy notwendig?

Es gibt heute eine Vielzahl existierender Techniken zur Dateiübertragung. Warum sollte mit envoy eine weitere eingeführt werden?

Standard-Protokolle zur Dateiübertragung

Zur Beantwortung dieser Frage haben wir einige der existierenden Technologien analysiert.

ftp

Eine Übertragung von Daten per ftp ist grundsätzlich unverschlüsselt. Für Angreifer ist es leicht, übertragende Daten sowie Benutzernamen und Passwörter abzufangen.

Die übertragenen Daten liegen unverschlüsselt auf dem Server, so dass sowohl befugte wie auch möglicherweise unbefugte Personen Zugriff auf die Daten haben können.

Durch manuelles Verschlüsseln der Daten und den Austausch von Passwörtern z.B. per Telefon lässt sich die Sicherheit verbessern. In der Praxis wird das aber aus Bequemlichkeitsgründen häufig unterlassen.

sftp/ftps

Diese Protokolle bieten im Gegensatz zu ftp eine Verschlüsselung der übertragenden Daten. Damit sind zumindest Benutzernamen und Passwörter sowie die übertragenen Daten für Angreifer nicht ohne weiteres abzufangen.

Allerdings betrifft die Verschlüsselung nur den Übertragungsweg. Die Daten selbst werden auf dem Server so abgespeichert, wie sie vom Absender gesendet wurden - in der Praxis meist unverschlüsselt. Damit bestehen auf dem Daten-Server die gleichen Sicherheitsprobleme wie bei ftp.

https

Dieses Protokoll kann direkt aus dem Internet-Browser verwendet werden, was den Einsatz zunächst sehr attraktiv erscheinen lässt, da keine Software-Installation notwendig ist - wir gehen davon aus, dass ein Internet-Browser Teil der Standard-Installation ist.

Ein Nachteil des Protokolls besteht jedoch darin, dass die Übertragung mehrerer Dateien gleichzeitig nur unzureichend unterstützt wird. Auch sehr große Dateien bereiten in der Praxis häufig Probleme, da temporäre Verbindungsunterbrechungen nicht ausreichend behandelt werden können.

Bei der Verschlüsselung selbst bestehen grundsätzlich die gleichen Probleme wie bei sftp/ftps.

Fazit

Zwar ist mit Standardprotokollen eine Verschlüsselung des Transportwegs möglich, auf dem Datenserver selbst liegen die Daten jedoch unverschlüsselt vor, wenn nicht zusätzliche Vorsorge getroffen wurde. Selbst bei einem verschlüsselten Dateisystem auf dem Server bleibt zwischen Transportverschlüsselung und Dateisystemverschlüsselung eine Lücke, die Angreifer ausnutzen können.

Verwaltung des Daten-Servers

Neben der eigentlichen Datenübertragung muss eine vollständige File-Transfer-Lösung auch die Verwaltung von Benutzern und Gruppen, die Datenintegrität, die Datenzustellung sowie das Life Cycle Management der übertragenen Daten implementieren.

Benutzer und Gruppen

Unabhängig vom Übertragungsprotokoll können Benutzerverwaltungen zum Beispiel über das Berechtigungs-System des Betriebssystems des Daten-Servers implementiert werden.

Für das Ablegen unverschlüsselter Daten kann dieses Vorgehen ausreichend sein. Für das Speichern von verschlüsselten Daten ist jedoch zusätzlich eine Schlüsselverwaltung notwendig, die mit diesen Bordmitteln nicht realisierbar ist.

Datenintegrität

Es ist wünschenswert, dass nur vollständig und korrekt übertragende Daten einer Weiterverarbeitung zugeführt werden. Bei den oben vorgestellten Protokollen sind jedoch keine Mechanismen vorgesehen, die das sicherstellen.

Sind mehrere Dateien zu übertragen, lässt sich zudem schwer feststellen, ob die komplette Übertragung aller Dateien abgeschlossen ist - es fehlt ein Transaktionskonzept.

In der Praxis lassen sich diese Unzulänglichkeiten durch Verwendung zusätzlicher Werkzeuge wie zum Beispiel eines ZIP-Archivs umschiffen. Es verbleibt jedoch das Problem, dass die Daten auf dem Daten-Server weiterhin unverschlüsselt abgelegt werden - ZIP-Passwörter sind hierbei nur eine trügerische Sicherheit, eine Industrie von Anbietern hat sich auf das Knacken dieses Schutzes spezialisiert.

Datenzustellung

Die Empfänger von Daten sollten z.B. per E-Mail oder eine Meldung auf dem Desktop über das Eintreffen neuer Daten informiert werden.

Life Cycle Management

Der Daten-Server ist nur eine Zwischenstation für die Daten. Wurden Daten zur Weiterverarbeitung vom Server abgeholt, sollte das System daher automatisch für die Freigabe des Speicherplatzes sorgen. Das automatische Entfernen von nicht mehr benötigten Daten hält das permanent vorzuhaltende Speichervolumen klein und steigert zudem die Sicherheit.

Fazit

Eine Teil dieser Anforderungen lässt sich auch durch entsprechende Implementation auf dem Daten-Server mit Hilfe der Standard-Protokolle und unter Zuhilfenahme einiger zusätzlicher Tools umsetzen. In der Praxis findet jedoch eine Lösung, die aus mehreren Komponenten aufgebaut ist keine Akzeptanz, da die Bedienung umständlich ist.

Daher resultiert auch, dass Benutzer selten alle Vorgaben zur Verschlüsselung konsequent umsetzen:

- Logins und Passwörter werden wie selbstverständlich per E-Mail durch die Welt gesendet
- Umständliche Benutzerverwaltungen führen häufig zu „Sammel-Logins“, die von mehreren Benutzern gleichzeitig verwendet werden

- Gast-Zugänge ermöglichen ungewollt Zugriff auf hochgeladene Daten anderer Benutzer

Wie envoy diese Probleme löst

Diese praktischen Erfahrungen haben daher zur Entwicklung von envoy geführt:

- einfache Verwendung auch für externe Benutzer
- konsequente, durchgängige und transparente Verschlüsselung
- flexible Steuerung der Daten-Zustellung
- einfache Administration

Ein Brief an die IT-Abteilung

envoy erfordert die Installation einer Software auf dem Rechner des Benutzers.

Warum? Nur auf diese Art und Weise können wir mit dem heutigen Stand der Technik eine sichere durchgängige Verschlüsselung und Unterbrechungstoleranz realisieren.

Die sicherlich wünschenswerte Implementation einer durchgängigen Verschlüsselung durch eine Web-Applikation scheitert heute noch an den gegebenen Limitierungen der gängigen Javascript-Implementationen. Dazu kommen Sicherheitsprobleme in den Browsern selbst.

Auch die Verwendung alternativer Verschlüsselungs-Techniken wie z.B. TrueCrypt erfordert die Installation zusätzlicher Software, löst dabei aber nur ein Teilproblem.

Wir sind daher der Meinung, dass die Installation einer zusätzlichen Anwendung in der Praxis kein Hindernis darstellen sollte, auch wenn uns die gängige Skepsis in IT-Abteilungen diesbezüglich bekannt ist.

Allergrössten Wert haben wir daher auf eine einfache Installation und natürlich auch auf eine problemlose Deinstallation gelegt.

Die Oberfläche der envoy Anwendung haben wir so einfach gestaltet, dass auch unerfahrene Anwender leicht damit umgehen können.

Das Paket-Konzept für Transaktionen

In envoy werden Daten immer als Paket versendet. Dabei kann ein Paket beliebig viele Dateien und Verzeichnisse enthalten. Auf diese Art und Weise setzen wir das Konzept der Transaktion um - erst eine vollständige Übertragung aller Daten eines Pakets wird als erfolgreich bewertet. Unvollständige Pakete sind für Empfänger bereits sichtbar, können jedoch noch nicht heruntergeladen werden.

Zusätzlich können weitere Informationen in Form von Meta-Daten an Pakete angehängt werden, die zum Beispiel bei der Weiterverarbeitung ausgewertet werden können. Diese Meta-Daten lassen sich als Formular für jeden Ordner frei definieren.

Für Benutzer mit entsprechender Berechtigung ist es einfach zu erkennen, ob und von wem Pakete bereits heruntergeladen wurden.

Verschlüsselung von Daten

Die Verschlüsselung der Daten erfolgt ohne weiteres Zutun des Benutzers direkt beim Absender. Die Informationen zur Entschlüsselung werden allen potentiellen Empfängern vollautomatisch und sicher zugestellt.

Empfänger können versendete Pakete anschließend herunterladen. Die Entschlüsselung erfolgt dabei auch für den Empfänger völlig transparent.

Durch dieses Verfahren liegen weder unverschlüsselte Paket-Daten noch Paket-Schlüssel auf dem envoy-Server. Die für die Entschlüsselung notwendigen Informationen befinden sich auf der Empfängerseite.

Damit wird selbst beim einem Einbruch in den envoy Server gewährleistet, dass keine Daten gestohlen werden können.

Workflow

Jedes Paket kann einen Workflow-Status zugewiesen bekommen. Diese sind für jeden Ordner frei konfigurierbar und können zum Beispiel als Feedback für externe Kunden eingesetzt werden.

Benutzerverwaltung

Administratoren des Daten-Servers können sehr einfach neue Benutzer erstellen, bearbeiten und löschen. Neue Benutzer erhalten automatisch eine E-Mail, die den Download-Link für den envoy-Client sowie einen Anhang mit den Registrierungs-Informationen enthält.

Nach Installation des Clients genügt ein Doppelklick auf den Anhang, um den Benutzer im System zu aktivieren. Ab diesem Zeitpunkt kann der neuen Benutzer bereits Daten per envoy versenden.

Die anschließende Zertifizierung des neuen Benutzers durch den Administrator schließt die Registrierung ab. Der neue Benutzer kann ab dann per envoy Daten auch empfangen.

Server-Verwaltung

Der Austausch von Daten erfolgt in envoy grundsätzlich über Ordner. Für diese Ordner kann ein Administrator unter anderem festlegen, welche Benutzer Pakete in den Ordner senden und welche Benutzer Pakete aus dem Ordner empfangen dürfen.

envoy bietet zudem pro Ordner umfangreiche Einstellmöglichkeiten, um den Verbleib von Daten auf dem Server zu regeln. So ist es zum Beispiel möglich, empfangene Pakete sofort oder nach einer einstellbaren Zeit automatisch zu löschen.

Automatisierung

Über die Zusatzkomponente envoy Robot ist es möglich, mit gängigen Scripting Sprachen wie z.B. python eine Automatisierung von Transfer-Abläufen durchzuführen.

Fazit

envoy implementiert die Anforderungen an ein modernes, sicheres und flexibles File-Transfer-System.

Alle Funktionen sind über ein einheitliches, schlankes Client-Programm zu steuern, dessen Oberfläche sich je nach Rolle des Benutzers anpasst: Von der minimalen Oberfläche für externe Benutzer bis zur vollständigen Funktionalität für Administratoren.

envoy im Internet

http://ww.envoy.de

Live-Demo: http://demo.envoy.de

Dokumentation: http://www.envoy.de/doc/de/admin/index.html