GoldBug (Instant Messenger)

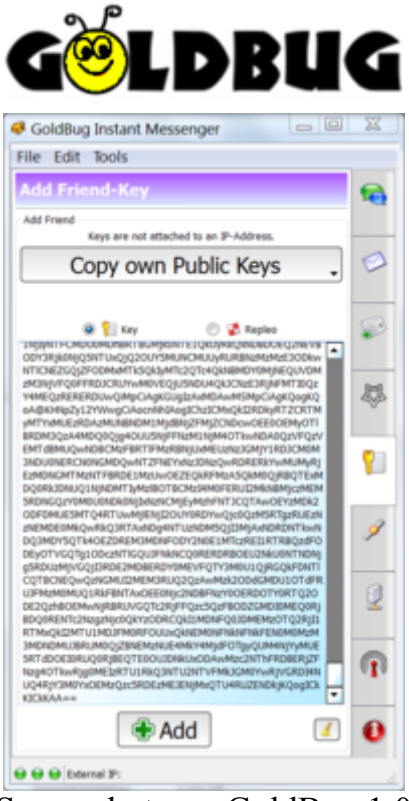
Aus MARJORIE-WIKI

GoldBug ist ein E-Mail-Programm und Instant Messenger sowie auch eine Internet-Suchmaschine basierend auf dem Protokoll *Echo* und dem Programmkern Spot-on. GoldBug nutzt dabei starke Mehrfach-Verschlüsselung (siehe: Hybride Verschlüsselung) mit verschiedenen Schichten von modernen Verschlüsselungs-Technologien von etablierten und auditierten Verschlüsselungs-Bibliotheken[1] (wie libgcrypt (bekannt von GnuPG) und OpenSSL – d. h. Implementierung nach RFC 4880 des OpenPGP-Standards bzw. Zertifizierung nach FIPS 140-2).

Das Programm beinhaltet als quelloffene Kommunikations-Suite weiterhin dezentrales und verschlüsseltes E-Mail und einen dezentralen öffentlichen e*IRC-Gruppen-Chat, welcher ebenso auf dem Echo-Protokoll basiert – also eine Art von *ge-echo-tem* IRC.[2] Ebenso ist ein Feedreader integriert.

Die Applikation erlaubt es, manuell und eigenständig seine persönlichen Verschlüsselungs-Komponenten auszuwählen z. B. mit Verschlüsselung durch RSA, NTRUEncrypt, Elgamal oder dem McEliece Algorithmus, der auch mit dem Modell nach Fujisaki-Okamoto gegen einen IND-CCA2 Angriff absichert ist.

GoldBug



Screenshot von GoldBug 1.0

Basisdaten	
Aktuelle Version	3.3 (01 Januar 2017)
Betriebssystem	Microsoft Windows, Mac OS X, Linux
Programmier-sprache	C++
Kategorie	E-Mail-Programm, Instant Messenger, Chat, E-Mail, Suchmaschine, Newsgroups, Filesharing,
Lizenz	BSD (Freie Software)

goldbug.sourceforge.net (http://goldbug.sourceforge.net/)

Die beiden Algorithmen NTRU und McEliece gelten als Quantum Computing resistent. Damit ist GoldBug einer der wenigen E-Mail-Klienten und Instant Messenger, der beide zukunftsicheren Algorithmen implementiert hat.

Ebenso können Schlüsselgröße, Cipher-Methode, Hash, Salt und Iteration individuell eingestellt werden.[3]

GoldBug ist eine Benutzeroberfläche für den Spot-on Echo-Kernel, der in C++ mit der Qt-Bibliothek geschrieben wurde. Das Programm ist verfügbar für Windows, Mac OS X und Linux, hier insbesondere FreeBSD, Debian und openSUSE.

Inhaltsverzeichnis

- 1 Namensherkunft
- 2 Verbindungs-Modi
  - 2.1 Volles Echo
  - 2.2 Halbes Echo
  - 2.3 Adaptives Echo
  - 2.4 Echo Accounts
- 3 Standards und Bibliotheken für die Verschlüsselung
- 4 Tabs und Grundfunktionen
  - 4.1 Chat
  - 4.2 E-Mail
  - 4.3 Poptastic
  - 4.4 e*IRC / Buzz als Gruppenchat
  - 4.5 StarBeam File Transfer
  - 4.6 URL Web-Suche
  - 4.7 Rosetta CryptoPad
  - 4.8 File-Encryption Werkzeug
  - 4.9 Serverloser Schlüsselaustausch
- 5 Ausgewählte Ausstattungen, Standards und Methoden
  - 5.1 Repleo
  - 5.2 E-Mail-Institutionen
  - 5.3 Magnet URI Verschlüsselungs Standard
  - 5.4 SMP: Socialist Millionaire Protokoll
  - 5.5 Echo Public Key Share (EPKS)
  - 5.6 Forward Secrecy
  - 5.7 Secret Streams
- 6 Auditierung und Evaluierung der Software
- 7 Versionsgeschichte
- 8 Vergleich mit ähnlichen Werkzeugen für Sichere Kommunikation
  - 8.1 Vergleich mit OTR
  - 8.2 Vergleich mit RetroShare

- 8.3 Vergleich mit YaCy
- 9 Siehe auch
- 10 Weblinks
- 11 Einzelnachweise

Namensherkunft

Der Name GoldBug geht zurück auf die Kurzgeschichte *Der Goldkäfer* von Edgar Allan Poe: Die Geschichte erzählt von William LeGrand, der letztens einen gold-farbigen Marienkäfer entdeckte. Sein Freund Jupiter fürchtete sodann, LeGrand sei nun durch den Kontakt mit dem Marienkäfer besessen in der Suche nach Schätzen, Erfahrungs-Wissen und Weisheiten – und geht zu einem weiteren alten Freund von LeGrand. Nachdem sie sodann eine geheime Botschaft entschlüsselt haben, beginnen die drei ein Abenteuer als Team. Edgar Allan Poes Kurzgeschichte und Ideen zur Kryptographie halfen ebenso, verschlüsseltes Schreiben und Kryptogramme seit 1843 bekannt zu machen. Der Name der Software bezieht sich somit über 170 Jahre später in symbolischer Weise auf diesen alten Kontext.

Verbindungs-Modi

Verbindungen im Echo-Protokoll des GoldBug-Messengers können in drei verschiedenen Modi betrieben werden: Volles Echo, Halbes Echo und Adaptives Echo. Weiterhin ist bei allen drei Methoden die Einrichtung eines Echo-Accounts möglich.

Volles Echo

Der Modus des Vollen Echos sendet jedes verschlüsselte Nachrichten-Paket an jeden verbundenen Nachbarn. Jeder Nachbar führt dieses ebenso durch. In kleineren Netzwerken wird so jeder Peer zeitgerecht erreicht. Ein Node kann dann im Clienten-Modus, im Server-Modus oder als sogenannter Servent betrieben werden, bei dem er zugleich ein Chat-Server als auch ein Chat-Teilnehmer-Client ist.

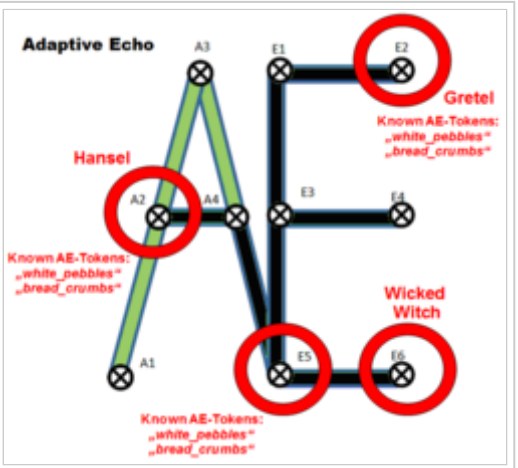
Halbes Echo

Das Halbe Echo sendet die Chat-Nachricht nur einen Hop weiter an den direkten Nachbarn bzw Chat-Freund. Das bedeutet, dass zwei Nachbarn miteinander Informationen austauschen können und die Nachricht nicht an weitere Teilnehmer ausgeliefert wird. Obwohl sowieso immer verschlüsselt, können mit dieser Methode des Halben Echos andere Teilnehmer im Netzwerk davon ausgeschlossen werden, dass sie überhaupt von der Nachrichtenübermittlung erfahren.[4]

Adaptives Echo

Das Adaptive Echo (AE) sendet die Nachricht – wenn entsprechende kryptographische Token vorhanden sind – ausschließlich nur zu den verbundenen Nachbarn, die ebenso den entsprechenden Verschlüsselungs-Token kennen. Die Abbildung an der Seite erläutert das Kommunikationsbeispiel von Hänsel und Gretel. Bezugnehmend auf das alte Märchen markieren beide Teilnehmer im Wald die Spur, um aus dem Wald wieder heraus zu finden – mit weißen Kieselsteinen und Brotkrumen. Sie möchten den Wald wieder verlassen und darüber kommunizieren, ohne dass die Böse Hexe davon Kenntnis erlangt. Wie können Hänsel und Gretel miteinander kommunizieren, ohne dass die Böse Hexe davon Kenntnis erlangt?

Die Teilnehmer in diesem Beispiel nutzen das Verschlüsselungs-Stichwort „Weiße Kieselsteine“. Die Nachricht wird dann nicht zu dem Peer der Bösen Hexe (Node E6) gesandt.[5] Alle anderen Teilnehmer, die den Verschlüsselungs-Token „Weisse Kieselsteine“ nicht kennen, verhalten sich regulär nach dem Vollen bzw. wenn definiert: Halben Echo (s.o.) und senden die Nachricht wiederum an alle bzw. nur den einen definierten, verbundenen Nachbarn.



Die Grafik zeigt das Adaptive Echo-Protokoll für echocasting. Mit Verschlüsselungs-Tokens lernen die einzelnen Computer im Netzwerk, an welche Teilnehmer eine Nachricht zu senden ist und an welche nicht.

Echo Accounts

Accounts definieren einfach eine Ausschließlichkeit im Verbinden zu einen anderen Peer oder Nachbarn. Node A und Node B können dann nur miteinander Verbinden, wenn sie zuvor sich auf genaue Accout-Logins und ein Passwort verständigt haben. Dieses erlaubt es, ein Web of Trust zu etablieren, ohne dass der öffentliche Verschlüsselungs-Key preisgegeben werden muss und ohne dass ein Verschlüsselungs-Key einer bestimmten IP-Adresse zugeordnet werden muss oder kann.

Standards und Bibliotheken für die Verschlüsselung

Neben RSA, Elgamal und NTRU nutzt das Programm GoldBug auch den Algorithmus McEliece. Als Verschlüsselungs-Bibliotheken werden u.a. libgcrypt (siehe GNU Privacy Guard) und OpenSSL eingesetzt. Die Nachricht eines Teilnehmers wird sodann verschlüsselt z.B. in dem folgenden Format: SSL (AES (RSA (Nachricht))).

Das bedeutet, die verschlüsselte Nachricht wird durch einen selbst-signierten SSL-Kanal zum anderen Nachbarn gesendet. Durch die Benutzung verschiedener Schichten von Verschlüsselung wird es einem Angreifer sehr schwer gemacht, die Verschlüsselung überhaupt brechen zu können.

Ebenso kann der sichere SSL-Kanal dazu genutzt werden, einen symmetrischen Schlüssel (siehe: Ende-zu-Ende-Verschlüsselung) zu senden, z. B. einen AES-Schlüssel. So werden Aufzeichnungen Dritter vermieden, die Schlüssel abfangen wollen, die im Klartext übertragen werden.

Die selbst-signierte Peer-to-Peer-SSL-Verbindung ist abgesichert gegen Man-In-The-Middle-Angriff des Transportweges durch verschiedene Maßnahmen wie z. B. optional die IP-Adresse des Nachbarn in das SSL-Zertifikat mit zu inkludieren oder auch durch die Möglichkeit, ein permanentes SSL-Zertifikat zu erstellen, so dass ein durch Dritte unbemerkt ersetzter, falscher Nachbar nicht in der Lage wäre, sich zu verbinden und dann sofort auffallen würde.[5]

Tabs und Grundfunktionen

Neben dem „Login“-Tab, um sich in die Benutzeroberfläche mit einer Passphrase, die mindestens 16 Zeichen umfassen muss, und dem „Add-Friend-Key“-Tab, bei dem der Verschlüsselungs-Key des Freundes eingegeben wird, hat das GoldBug Proframm verschiedene weitere Funktionen, unter anderem: Chat, E-Mail, Gruppenchat (auch e*IRC oder Buzz genannt) sowie Datei-Transfer (hier StarBeam FileSharing genannt).

Chat

Chat-Nachrichten in GoldBug sind immer verschlüsselt. Neben der Verschlüselungsmethode nach RSA oder Elgamal kann auch eine Verschlüsselung mit einem symmetrischen Schlüssel (wie z. B. AES) genutzt werden. Der symmetrische Schlüssel kann manuell eingegeben werden (z. B. wenn man sich auf ein Passwort einigt, das die Stadt benennt, in der man geheiratet hat) oder er kann auch automatisch generiert werden im AES Standard mit 32 zufälligen Zeichen. Der symmetrische Schlüssel wird dann zusätzlich noch abgesichert mit einem MAC Hash. Ein Nutzer, der das Verschlüsselungsverfahren Elgamal verwendet, kann ebenso mit einem Nutzer chatten, der das Verschlüsselungsverfahren RSA anwendet.[5]

E-Mail

GoldBug enthält auch einen funktionablen E-Mail-Klienten. Dieses ermöglicht es, E-Mails über eine Peer-to-Peer-Methode zu senden, ohne einen zentralen POP3- oder IMAP-Server in Anspruch zu nehmen.[5] Seit der Version 1.8 ist auch ein voller E-Mail-Klient für POP3 und IMAP basierend auf der Bibliothek LIBCURL integriert. Damit

kann E-Mail sowohl verschlüsselt als auch in offenem Text Modus empfangen und gesendet werden. GoldBug ist damit neben Trojita eine Alternative zu einem E-Mail-Klienten, der quelloffen das QT Framework von Digia nutzt.

Poptastic

Poptastic ist ein verschlüsselter Chat auf Basis von E-Mail. Die E-Mails werden Ende-zu-Ende asymmetrisch – und hybride ergänzend symmetrisch – verschlüsselt. Poptastic ist proxy-fähig und kann daher auch hinter einer Firewall oder über Tor betrieben werden.

e*IRC / Buzz als Gruppenchat

Der Gruppen-Chat is ebenso immer verschlüsselt. Er wird e*IRC (*ge-echo-ter* IRC) oder Buzz genannt, was der Original-Name im Spot-on Klienten, Kernel und Quellcode ist. Diese Art des Gruppen-Chats erfordert es nicht, dass die Teilnehmer öffentliche Schlüssel aus dem Paar öffentlicher und privater Schlüssel tauschen. Der e*IRC ist basierend auf dem Magnet-URI-Standard und jeder der den Magneten kennt, kann den Chat entschlüsseln und daran teilhaben (siehe auch weiter unten die Erläuterung des Magnet URI Standards für Verschlüsselung).[5]

StarBeam File Transfer

StarBeam ist die Funktion und das entsprechende Tab, um eine Datei in Form von verschlüsselten Paketen über das Internet zu senden. Jeder, der den Magnet-Link kennt, wird in der Lage sein, die Datei zu entschlüsseln. Um zu vermeiden, dass Magneten in die Öffentlichkeit gegeben werden, kann zusätzlich ein sogenanntes „Nova“-Passwort auf die Datei gesetzt werden – so dass das Nova-Passwort erst zu einem späteren Zeitpunkt freigegeben werden kann, z. B. wenn der Transfer schon längst abgeschlossen ist. Das Nova ist eine zweite Schicht an Verschlüsselung, neben der Einführung des Magnet URI Standards für Verschlüsselung im Quellcode des Spot-on-Kernels.[5]

URL Web-Suche

Seit der Version 2.5 ist eine p2p Websuche in einer URL-Datenbank integriert. Nutzer können über den Web Browser Dooble und weiteren Importfunktionen eine Websuche in einer peer-to-peer verteilten URL-Datenbank durchführen. Die Datenbank ist wie auch der Transfer der URLs vollständig verschlüsselt. Die Suchworte der Websuche werden daher nicht dem Zugriff von Dritten ausgesetzt. Seit Version 2.8 steht auch ein Webcrawler namens *Pandamonium* als zusätzliches Werkzeug zur Verfügung, mit dem die eigene URL-Datenbank neben dem p2p-Transfer der URLs von Freunden gefüllt

werden kann. Seit Version 2.9 wurde auch ein Feedreader ergänzt, mit dem Web-Feeds im Format RSS oder Atom in einer Timeline eingesehen werden können und weitergehend auch für die URL-Websuche importiert werden können.

Rosetta CryptoPad

Das Rosetta CryptoPad ist eine weitere Funktion as pop-up-Werkzeug, um Klartext in Chipertext umzuwandeln. Ebenso basierend auf einem Paar von öffentlichem und privatem Schlüssel können Nutzer den verschlüsselten Text dann über herkömmliche Klartext-Protokolle wie @-mail oder über jedes andere Nachrichtenprogramm austauschen; auch in Foren kann der Text gepostet und sodann vom Freund wieder ausgelesen und decodiert werden. So wird eine Art „slow-chat“ durchgeführt, da jeder die Nachricht erst manuell ver- und entschlüsselt.[5] Der Name Rosetta CryptoPad geht zurück auf den Stein von Rosette, welcher früher als eine Art Übersetzungs-„Buch“ für ägyptische Hieroglyphen diente. Dieses kleine Pad als Verschlüsselungs-Werkzeug wurde erstmals in der Version 0.8 als Weihnachtsveröffentlichung in 2013 vorgestellt.

File-Encryption Werkzeug

Seit der Version 1.0 von GoldBug ist ein Werkzeug integriert, dass es ermöglicht, eine Datei in eine verschlüsselte Datei umzuwandeln. Dazu kann der Nutzer den Chiper-Verschlüsselungsalgorithmus, Hash, Vektoren und eine Signierung wählen. Es ermöglicht somit, z. B. potentiell unsichere Container von TrueCrypt mit einer weiteren Verschlüsselungsschicht zu versehen oder auch Dateien, die in eine Dropbox oder zu einem Filehoster wie Megaupload hochgeladen werden sollen, vorab zu verschlüsseln. Natürlich kann damit auch ein Anhang einer E-Mail oder eine Datei für einen Transportweg innerhalb von GoldBug z. B. über die FileSahring-Funktion StarBeam verschlüsselt werden.

Serverloser Schlüsselaustausch

Mit der Version 2.5 wurde von GoldBug auch der serverloses Schlüsselaustausch veröffentlicht. Während PGP-Key-Server, die bislang ein zentrales Modell für eine Suche nach Schlüsseln zur Verschlüsselung darstellten, wurden in ein serverloses Paradigma mit einem Schlüsseltausch über das Echo-Protokoll innoviert. Die Nutzer setzen dabei einen 16-Zeichen langen Community-Namen fest und können darüber nun Ihre Schlüssel anderen Nutzern ebenso zur Verfügung stellen, die ebenso diesen Community-Namen kennen und wählen.

Ausgewählte Ausstattungen, Standards und Methoden

GoldBug hat eine Vielzahl an kryptographischen Ausstattungen und Features wie die Auswahlmöglichkeit verschiedener Verschlüsselungs-Algorithmen, auch als Multi-Encrpytion oder Hybride Verschlüsselung zusammengefasst. Weitere Haupt-Funktionen des Programms sind verschlüsselter Gruppenchat, das Senden von Schlüsseln nicht im Klartext, sondern im verschlüsselten Zustand des Ciphertextes, Ende-zu-Ende Verschlüsselung, öffentliche quasi IRC-Räume mit Verschlüsselung, integriertes BitMail als E-Mail-Klient (in Form von Peer-to-Peer-E-Mail), die Möglichkeit, mit dem Messenger über das Netzwerk Tor zu chatten, instant forward secrecy, das Aussenden von zufälligen Falschnachrichten, um ungebetene Lauscher zu verwirren, die Option zu authentifiziertem Chat und viele andere Optionen.[6]

Repleo

In GoldBug besteht die Möglichkeit, den eigenen, öffentlichen Verschlüsselungs-Key ebenso über verschlüsselten Chiphertext zurückzusenden, ihn also nicht im Klartext zu senden – wenn der Freund seinen öffentlichen Schlüssel zuerst geschickt hat. Dieses wird dann Repleo genannt.[7] Ebenso ermöglicht es das integrierte E-Mail-Programm, dass der Chat-Verschlüsselungs-Key z. B. in einer verschlüsselten Weise über E-Mail versandt wird.

E-Mail-Institutionen

Die E-Mail-Funktion von GoldBug basiert auf einem puren Peer-to-Peer-E-Mail. Das versenden einer E-Mail an einen Partner, der offline ist, kann in dem peer-to-peer Netzwerk über zwei Methoden durchgeführt werden. Einmal: Wenn beide Freunde einen dritten gemeinsamen Freund haben und alle ihre Verschlüsselungs-Keys austauschen – z. B. wenn Alice und Bob beide einen gemeinsamen dritten Webserver nutzen und sie die Verschlüsselungs-Keys austauschen, dann wird der Webserver die E-Mails zwischenspeichern für den Freund, der derzeit offline ist. Das funktioniert natürlich auch, wenn der Webserver ein realer dritter Freund ist, der kontinuierlich online ist. Oder, zweite Methode: eine sogenannte E-Mail-Institution wird erstellt. Für diese Instanz wird einen spezieller Verschlüsselungs-Magnet-URI erstellt. Wenn der Magnet bei den Nutzern bekannt ist und die E-Mail-Institution die Verschlüsselungs-Keys der Nutzer abgespeichert hat, dann werden die E-Mails in dieser Art einer virtuellen Institution zwischengespeichert. Der Verschlüsselungs-Key des Nutzers, der die E-Mail-Institution einrichtet, muss nicht heraus- oder bekannt gegeben werden, lediglich der Magnet der E-Mail-Institution muss bei den anderen Nutzern bekannt und eingegeben sein.[5] Und, wie genannt, der Ersteller einer E-Mail-Institution gibt den Verschlüsselungs-Key eines Nutzers der Institution in die Institution ein. Sodann können auch E-Mails abgerufen werden aus einer Institution mit der man nicht direkt, sondern P2P verbunden ist.

Magnet URI Verschlüsselungs Standard

Der Magnet-URI-Standard wurde ausgearbeitet und weiterentwickelt in ein Format, um Verschlüsselungswerte ähnlich einem Blatt mit Blutwerten weiter geben zu können. Ein Magnet-URI, der in GoldBug, respektive für den Spot-On Entwickler Gruppen-Chat-Kanal genutzt wird, sieht aus wie in diesem Format:

- magnet:?rn=Spot-On_Developer_Channel_Key&xf=10000&xs=Spot-On_Developer_Channel_Salt&ct=aes256&hk=Spot-On_Developer_Channel_Hash_Key&ht=sha512&xt=urn:buzz

und die Kategorien sind wie folgt abgekürzt:

- rn=Spot-On_Developer_Channel_Key& = Raum Name
- xf=10000& == Exacte Frequenz
- xs=Spot-On_Developer_Channel_Salt& = Exactes Salz
- ct=aes256& = Cipher Type // Chiffrierungs Typ
- hk=Spot-On_Developer_Channel_Hash_Key& = Hash Key
- ht=sha512& = Hash Type (z. B. SHA or Whirlpool)
- xt=urn:buzz = Die Extension ist Buzz, ein neues Wort für e*IRC oder einen Gruppen-Chat Raum, basierend auf dem Echo-Protokoll

Dieser Standard wird genutzt, um symmetrische Schlüssel zu tauschen für Gruppenchat oder E-Mail-Institutionen oder auch Dateiübertragungen mit StarBeam.[5]

SMP: Socialist Millionaire Protokoll

Das Socialist Millionaire Protokoll[8] ist seit der Version 1.9 in GoldBug integriert und ermöglicht eine alternative Authentifizierung des Chat-Partners. SMP wird auch im OTR bei XMPP genutzt. Beide Chat-Partner müssen dazu ein einfaches Passwort eingeben, um sich gegenseitig zu authentifieren: wie beispielsweise der Name des Restaurants, in dem beide sich das erste Mal getroffen haben oder die Stadt, in der sie geheiratet haben. Somit wird sichergestellt, dass am anderen Ende auch wirklich der erwartete Chat-Partner ist. Die Eingaben für das Authentifizierungs-Password kann seit der Version 2.1 über ein virtuelles Keyboard erfolgen, um Keyloggern das Speichern von Passphrasen zu unterbinden. Das Keyboard ist in deutscher und englischer Sprache verfügbar und funktioniert über Doppelklick nicht nur bei der SMP-Eingabe, sondern bei jeglicher Authenifizierungsabfrage des Messengers, also auch beim Initial-Login.

Echo Public Key Share (EPKS)

Mit der Funktion Echo Public Key Share (EPKS) (seit Release 2.6) können die üblichen Key-Server, auf denen die Schlüssel von Nutzern gesucht werden können, ersetzt werden. Bei dem Echo Key Share wird in dem oben beschriebenen und der Applikation GoldBug zugrundeliegenden Echo Protokoll ein verschlüsselter Kanal durch ein symmetrisches, also ende-zu-ende verschlüsseltes Passwort erstellt. Dieses ist ein

Community-Name. Alle Online-Personen, die diesen Community-Namen kennen und eingegeben haben, erhalten dann von einem Nutzer seinen öffentlichen Schlüssel, wenn er diesen an die Community sendet. So kann beispielsweise ein Communityname "Waldorfschule" genutzt werden, damit alle Personen, die diesen Communitynamen eingegeben haben, von den Teilnehmer dieser Community den öffentlichen Schlüssel zugesandt bekommen. Standardmäßig ist eine Community beim Start der Applikation eingerichtet - und zwar für den automatischen Tausch des URL-Keys. Damit nimmt der Nutzer an der p2p Websuche des Klienten teil, indem er automatisch mit allen verbundenen Nutzern den URL-Key tauscht und dann auch in einem distribuierten URL-Netzwerk eine Websuche umsetzen kann, wie man es von YaCy z. B. kennt. Das Verfahren bietet dementsprechend gute Perspektiven, wesentlich sicherer den Tausch von Schlüssel über diese etablierten Online-Echo-Communities abzubilden.

Forward Secrecy

Während in der Chat Funktion Perfect Forward Secrecy über die Calling Funktion bereits mit symmetrischen Schlüsseln (z. B. ein Passwort oder eine AES-Zeichenfolge) vorhanden war unter den neuen Paradigma des Instant Forward Perfect Secrecy (IPFS), wurde mit der Veröffentlichung der Version 2.7 sowohl für Chat als auch für E-Mail nun Forward Secrecy (FS) auch mit asymmetrischen Schlüsseln ergänzt. Damit kann über den permanenten Schlüssel für Chat oder Email auch ein sitzungsbasiertes, also temporäres Schlüsselpaar eingerichtet werden, über das die Kommunikation dann abläuft. GoldBug ist damit weltweit der erste E-Mail-Client, der Forward Secrecy, also instant und sitzungsbasierte Schlüssel, sowohl zur asymmetrischen als auch symmetrischen Verschlüsselung für E-Mail und Chat anbietet.

Secret Streams

Mit dem Secret Streams Release in 2017 wurde die sog. Secret Streams Funktion hinzugefügt. Sie ermöglicht das Vorhalten von ephemeralen Sitzungsschlüsseln im Bereich des Konzeptes des Instant Perfect Forward Secrecy für Chat und als auch für E-Mail, die sich aus einem gemeinsam definierten, aber nicht online geteilten Geheimnis eines Socialist-Millionaire-Protokol-(SMP)-Prozesses ableiten. Gegenüber anderen Konzepten wie dem Signal-Protokoll mit seinem Double-Ratchet ist nunmehr bei GoldBug ergänzend sichergestellt, dass die in der Timeline befindlichen ephemeralen Sitzungsschlüssel authentifiziert sind mittels SMP. Damit ist der Fall ausgeschlossen, dass jemand Alice ihr Device aus der Hand nimmt und unter ihren temporären Schlüsseln jederzeit weiter kommunizieren kann. Secret Streams ist somit authentifiziertes Instant Perfect Forward Secrecy in einem Stream von Schlüsseln über das SMP-Fenster für E-Mail und Chat.

Auditierung und Evaluierung der Software

Die beiden Sicherheitsforscher David Adams (Tokyo) und Ann-Kathrin Maier (München) haben in ihrer BIG SEVEN Studie die sieben bekanntesten Verschlüsselungsprogramme für E-Mail und Chat-Nachrichten aus dem Open Source Bereich untersucht und sodann vertieft ein IT-Audit für die bekannte Software-Lösung GoldBug.sf.net durchgeführt. Das Audit berücksichtigte die wesentlichen Kriterien, Untersuchungsfelder und Methoden in Anlehnung an acht internationale IT-Audit Manuale und wurde in 20 Dimensionen durchgeführt.

Die Software „GoldBug - E-Mail-Programm und Instant Messenger“ hatte dabei excellente Bewertungen und zeigt sich nicht nur sehr vertrauenswürdig und compliant bzw. konform zu den internationalen IT-Audit-Manualen und Sicherheitsstandards. GoldBug punktet auch im Vergleich und der Bewertung der Einzelfunktionen wesentlich ausführlicher als die vergleichbaren anderen open source Crypto-Messenger. Die Münchener Co-Autorin der Studie Ann-Kathrin Maier ergänzt: *"Wir haben sodann unsere Messenger-Studie vertieft mit einem ausführlichen Audit des Crypto-Programms GoldBug, das excellente Ergebnisse für verschlüsseltes E-Mail und sicheren Online-Chat erhielt. Durch unsere Code-Reviews von GoldBug können wir die Vertrauenswürdigkeit in die Sicherheit dieser Open Source Verschlüsselung bestätigen.*"[9] Zahlreiche Details wurden durch verschiedenste Methoden analysiert, verglichen und auch von den beiden Autoren strategisch für die aktuellen Verschlüsselungs-Diskussionen bewertet. Zu den vergleichend untersuchten Applikationen zählen CryptoCat, GoldBug, OTR-XMPPKlienten wie z.B. Pidgin mit dem OTR-Plugin, RetroShare sowie Signal, Surespot und Tox.

Versionsgeschichte

- GoldBug V 2017.01.01_3.3 wurde veröffentlicht am 01. Januar 2017: Secret-Streams-(SMP-IPFS)-Release.
- GoldBug V 3.2 wurde veröffentlicht am 05. November 2016: Fujisaki-Okamoto Release.
- GoldBug V 3.1 wurde veröffentlicht am 12. Oktober 2016: McEliece Release.
- GoldBug V 3.0 wurde veröffentlicht am 28. August 2016: Threefish Release.
- GoldBug V 2.9 wurde veröffentlicht am 24. Januar 2016: RSS/Atom-Newsreader Release.
- GoldBug V 2.8 wurde veröffentlicht am 25. Dezember 2015: Pandamonium Webcrawler Release.
- GoldBug V 2.7 wurde veröffentlicht am 26. September 2015: Forward Secrecy in Email & Chat Release.
- GoldBug V 2.6 wurde veröffentlicht am 1. August 2015: Serverless Key Sharing Release.
- GoldBug V 2.5 wurde veröffentlicht am 19. Juni 2015: URL Websearch Release.
- GoldBug V 2.1 wurde veröffentlicht am 20. April 2015: Virtual Keyboard Release.
- GoldBug V 1.9 wurde veröffentlicht am 23. Februar 2015: Socialist-Millionaire-

Protocol (SMP) Release.
- GoldBug V 1.8 wurde veröffentlicht am 25. Januar 2015: E-Mail-Client-Release: Plaintext-Emails over POP3/IMAP.
- GoldBug V 1.7 wurde veröffentlicht am 6. Dezember 2014: Poptastic-XMAS-Release: Encrypted chat over POP3.
- GoldBug V 1.6a wurde veröffentlicht am 9. November 2014: 2-Way-Instant-Perfect-Forward-Secrecy: „2WIPFS“-Release.
- GoldBug V 1.5 wurde veröffentlicht am 10. Oktober 2014: Alternative Login Method Release.
- GoldBug V 1.3 wurde veröffentlicht am 30. September 2014: NTRU Release.
- GoldBug V 1.1 wurde veröffentlicht am 9. September 2014: Vector Update Release
- GoldBug V 1.0 wurde veröffentlicht am 7. September 2014: File Encryption Release.
- GoldBug V 0.9.09 wurde veröffentlicht am 21. August 2014: Smiley Release.
- GoldBug V 0.9.07 wurde veröffentlicht am 13. Juli 2014: Adaptive Echo Release.
- GoldBug V 0.9.05 wurde veröffentlicht am 31. Mai 2014: Added Example Project Chat Server Release.
- GoldBug V 0.9.04 wurde veröffentlicht am 22. April 2014: SCTP & Institution Release.
- GoldBug V 0.9.02 wurde veröffentlicht am 13. März 2014: StarBeam Analyzer Release.
- GoldBug V 0.9.00 wurde veröffentlicht am 7. Februar 2014: Tablet Gui Release.
- GoldBug V 0.8 wurde veröffentlicht am 23. Dezember 2013: Rosetta CryptoPad Release.
- GoldBug V 0.7 wurde veröffentlicht am 19. Dezember 2013: StarBeam Filesharing Release.
- GoldBug V 0.6 wurde veröffentlicht am 24. Oktober 2013: El-Gamal Release.
- GoldBug V 0.5 wurde veröffentlicht am 16. September 2013: Signature-Keys Release.
- GoldBug V 0.4 wurde veröffentlicht am 3. September 2013: Kernel-Improvement Release.
- GoldBug V 0.3 wurde veröffentlicht am 26. August 2013: Geo-IP-Release.
- GoldBug V 0.2 wurde veröffentlicht am 22. August 2013: SSL-Release.
- Goldbug V 0.1 wurde am 27. Juli 2013 veröffentlicht, basierend auf der Veröffentlichung am gleichen Tag des Echo/Chat Kernel Servers und Application, zurückgehend auf ein anderes, vorheriges Forschungsprojekt.

Vergleich mit ähnlichen Werkzeugen für Sichere Kommunikation

Vergleich mit OTR

OTR bietet ebenso über das XMPP-Chat-Protokoll Ende-zu-Ende-Verschlüsselung an. Im Vergleich ist hier die Verschlüsselung eine Aushandlung, die einmal pro Online-Sitzung erfolgt, während die Echo-basierten Chat-Applikationen dieses jede Sekunde erneuern oder randomisieren können. Das Kriterienmerkmal von perfect forward secrecy wurde weiterentwickelt zum Anspruch des *Instant* Forward Perfect Secrey (IFPS).[5] Während OTR ein Plug-in ist, sieht das Echo Protocol einen nativen, originären verschlüsselten Nachrichtentausch vor, ohne die Notwendigkeit, in der Software eine Plugin-Entwicklung (mit allen Schnittstellenoptionen und Sicherheitsüberlegungen) umsetzen zu müssen. Weiterhin ist das Socialist Millionaire Protokoll[8] (SMP) in beiden Chat-Verschlüsselungen bzw. -Clienten enthalten.

Vergleich mit RetroShare

RetroShare nutzt lediglich einen Schlüssel für alle Funktionen der Applikation, hat kein Messaging zu Freunden, die gerade offline sind, und korreliert die IP-Adresse zum Verschlüsselungs-Key – was in einer genutzten DHT und dem vorhandenen öffentlich bekannten Schlüssel schnell dazu führen kann, dass die eigene IP-Adresse herausgefunden und analysiert werden kann. GoldBug nutzt dementsprechend 8 verschiedene Verschlüsselungs-Keys für die verschiedenen Funktionen und erlaubt es auch, Nachrichten an Nutzer zu senden, die derzeit offline sind. Die Verschlüsselungs-Keys sind nicht an die eigene IP-Adresse korreliert, da die Regelung der Verbindungen der Freunde z. B. über Echo-Accounts geregelt werden kann, was weiterhin die Erstellung eines Web of Trusts ermöglicht. Aber auch im P2P-Modus sind die Keys nicht einer definierten IP-Adresse zuzuordnen. IP-Adressen können noch weitergehend auch dadurch vom Verschlüsselungs-Key separiert werden, indem die technischen Voraussetzungen optional vorhanden sind, das Netzwerk Tor mit dem GoldBug Messenger als eine Art TorChat zu nutzen.[5]

Vergleich mit YaCy

YaCy ist eine p2p Suchmaschine für URLs, die Suchergebnisse aus einem distribuierten Datenbestand zusammenstellt. GoldBug hat seit der Version 2.5 ebenso eine URL-Websuche integriert, und stellt somit eine Alternative in der p2p Websuche da, die im Vergleich zu YaCy Suchanfragen, Datentransfers und Speicherung der Datenbestände verschlüsselt. Zusätzlich wird durch die Verschlüsselung auch kein sogenannter "Queryhit" bei den Suchanfragen im Netzwerk generiert, wie es bei YaCy der Fall ist, so dass auch die Suchworte des Nutzers nicht durch Dritte oder Peers erfasst und ausgewertet werden können. Die Benutzeroberfläche ist Klienten-basiert und derzeit nicht browserbasiert.

Siehe auch

- Friend-to-friend
- Turtle F2F
- RetroShare
- GNUnet
- YaCy

Weblinks

- Offizielle Website (http://goldbug.sourceforge.net/)

Wikibooks: Deutsches Benutzerhandbuch für GoldBug

Einzelnachweise

1. *GoldBug uses crypto libraries (like libgcrypt (GnuPG) and OpenSSL*. (http://download.cnet.com/GoldBug-Instant-Messenger/3000-2150_4-75999130.html)
2. *The program GoldBug includes an encrypted mail component, as well as an IRC chat*. (http://www.softpedia.com/get/Internet/Chat/Instant-Messaging/GoldBug-Instant-Messenger.shtml) softpedia.com
3. *Secure chat communications suite GoldBug*. (http://www.hacker10.com/other-computing/secure-chat-communications-suite-goldbug/) Security Blog, 25. März 2014
4. Jan Weller: Testbericht zu GoldBug (http://www.freeware.de/download/goldbug_76583.html) für Freeware, Freeware-Blog
5. GoldBug Instant Messenger User Manual German (https://de.wikibooks.org/wiki/Goldbug) sourceforge.net
6. *Secure chat communications suite GoldBug*. (http://www.hacker10.com/other-computing/secure-chat-communications-suite-goldbug/) Security Blog, 25. März 2014
7. *GoldBug kann Schlüssel selbst encodiert versenden*. (http://www.heise.de/download/goldbug-1192605.html) heise.de
8. *Socialist Millionaire Protokoll* in der englischsprachigen Wikipedia
9. Adams, David / Maier, Ann-Kathrin (2016): BIG SEVEN Study, open source crypto-messengers to be compared - or: Comprehensive Confidentiality Review & Audit of GoldBug, Encrypting E-Mail-Client & Secure Instant Messenger, Descriptions, tests and analysis reviews of 20 functions of the application GoldBug based on the essential fields and methods of evaluation of the 8 major international audit manuals for IT security investigations including 38 figures and 87 tables., URL: https://sf.net/projects/goldbug/files/bigseven-crypto-audit.pdf - English / German Language, Version 1.1, 305 pages, June 2016

Dieser Wikipedia-Artikel wurde, gemäß GFDL, CC-by-sa (http://creativecommons.org/licenses/by-sa/3.0/legalcode.de) mit der kompletten History (https://marjorie-wiki.de/w/index.php?title=GoldBug_(Instant_Messenger)&action=history) importiert.

Abgerufen von „https://marjorie-wiki.de/w/index.php?title=GoldBug_(Instant_Messenger)&oldid=1704287“

Kategorien: Freie E-Mail-Software | Freie Instant-Messaging-Software | Freie Peer-to-Peer-Software | Instant-Messaging-Protokoll | Freie Kryptosoftware | Kryptologischer Standard | Qt | Linux-Software | Windows-Software | BSD-Software | Mac-OS-Software | OS/2-Software

---

- Diese Seite wurde zuletzt am 5. Januar 2017 um 19:23 Uhr geändert.
- Der Text ist unter der Lizenz "Creative Commons" „Namensnennung – Weitergabe unter gleichen Bedingungen“ verfügbar. Zusätzliche Bedingungen können gelten. Einzelheiten sind in den Nutzungsbedingungen beschrieben.