DER ANGRIFF AUF JABBER.RU

UND WAS WIR DAGEGEN TUN KÖNNEN

Daniel Gultsch

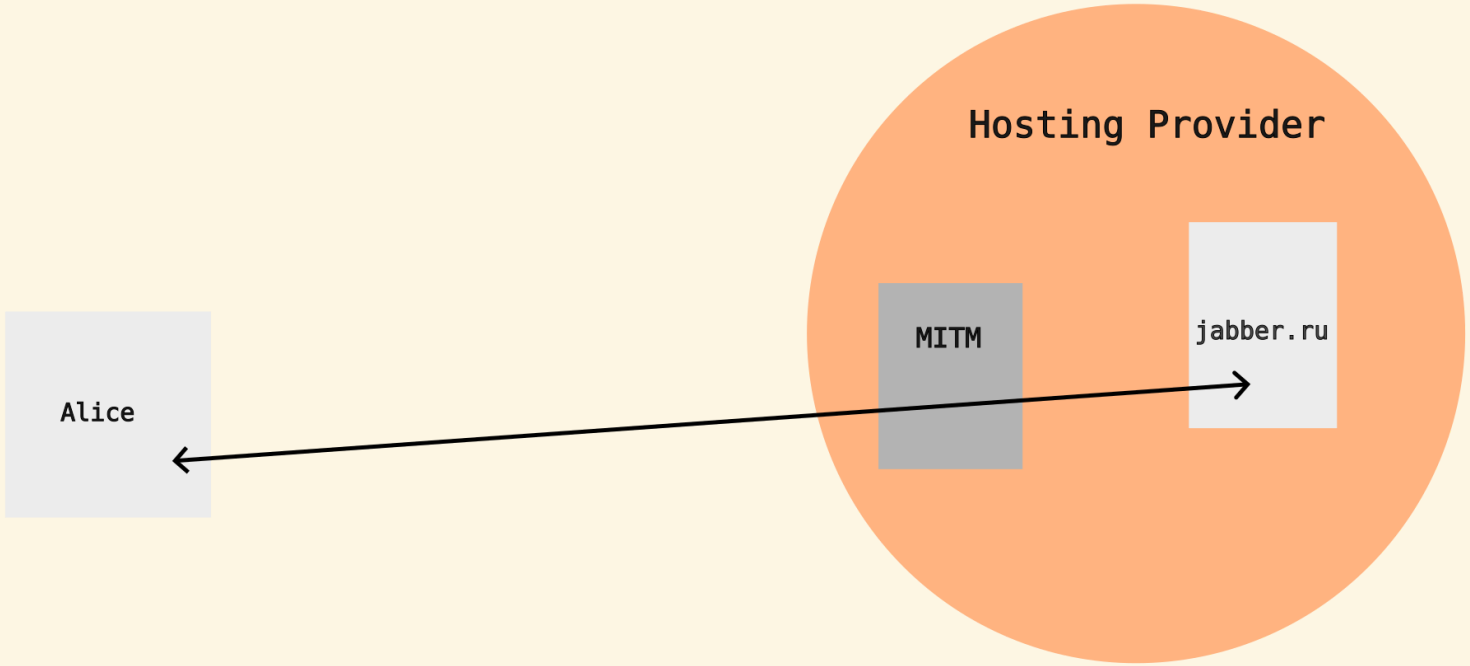
December 13th, 2023

DISCLAIMER

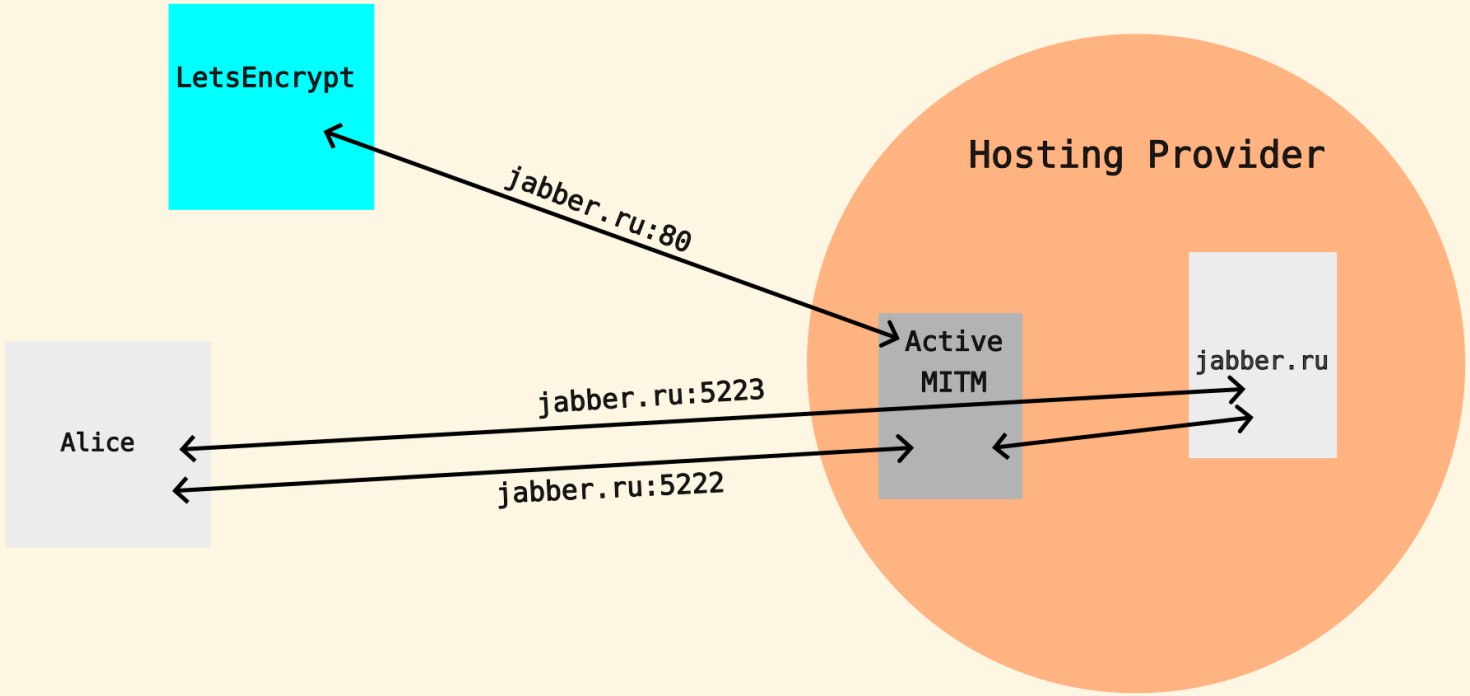
- Die angebliche Attacke[1] könnte komplett fingiert sein
  - Relativ detailierte und aufwendige Fälschung (tcpdumps + E-Mails an den Provider)
  - Unklares Ziel (der Fälschung)
- Wir wissen nicht wer es war

[1]: https://notes.valdikss.org.ru/jabber.ru-mitm/

PASSIVE MITM



ACTIVE MITM


LetsEncrypt
jabber.ru:80
Hosting Provider
Active
MITM
jabber.ru
Alice
jabber.ru:5223
jabber.ru:5222

WIE ERKENNEN WIR DAS?

- TCP/TLS Verbindung zwischen Client und MITM ≠ Verbindung MITM Server
  - TTL anders
  - Andere source ports
  - Anderes Client Hello (ciphers, random bytes)
- +1 hop für passive MITM ports (22, 5223)

TLS CERTIFICATES?

Aber sollten TLS certificates nicht belegen das wir mit jabber.ru reden?

TLS CERTIFICATES!

- ACME challenge trivial abzufangen wenn man zwischen Letsencrypt Server und jabber.ru sitzt.
- MITM proxy stellt sich selber certificates aus…

AUFGEFLOGEN

- … bis der Praktikant vergisst das certificate zu verlängern

CAA RECORDS

- DNS records die besagen das für die (sub) domain nur ein bestimmter ACME account certificates ausstellen kann
- Ggf zusätzlich auch Methode (DNS, HTTP)
- snikket.org/blog/on-the-jabber-ru-mitm

CERTIFICATE TRANSPARENCY

- CA trägt jedes ausgestellte Certificate in ein öffentliches log ein
- Client prüft das das geschehen ist
- Server Betreiber durchsucht öffentliche logs nach seiner Domain

EXKURS: SCRAM

- Standard Authentifizierung in XMPP[2]
- Client und Server beweisen sich gegenseitig das sie das Passwort kennen
- Passwort nicht übermittelt → Server nicht in der Lage sich als User auszugaben

[2]: PLAIN existiert für seltene Einsätze

SCRAM-PLUS (CHANNEL BINDING)

- Passwort + etwas Eindeutiges aus der TLS Verbindung

CHANNEL BINDING METHODEN

- Unique (TLSv1.2)
- Exporter (TLSv1.3)
- Endpoint (certificate hash)[3]

[3]: schützt nicht vor gestohlenen Certificates

XEP-0440

- SASL/SCRAM kann nur raten
- Welche Methoden kann mein Server

SOFTWARE SUPPORT

- Clients
  - Conversations + forks
  - Monal
- Server
  - Prosody (trunk)
  - ejabberd (trunk)

ZUSÄTZLICHE HINWEISE

- `endpoint` ist so semi secure
- Passwort geheim halten!

DANKE!

gultsch.de · daniel@gultsch.de · @daniel@gultsch.social