Demo of DANE-Enhanced Version of “Off-the-Record” Private Messaging Tool

Bootstrapping Trust for “Off-The-Record” With DNS and DNSSEC

Allison Mankin (Verisign Labs), Willem Toorop (NLNet Labs),
Iain Learmonth (University of Aberdeen),
Sathya Gunesekaran (Georgia Tech)

ICANN DNSSEC Workshop
25th June 2014

getdnsapi

- getdns is a modern asynchronous DNS API
- getdns performs DNSSEC validation of records returned
- getdns allows applications to access DNSSEC validation

dnskeys

- dnskeys is a Python library that fetches public cryptographic keys from DNS and validates their authenticity using DNSSEC
  - RFC6698 (TLSA)
  - draft-wouters-dane-openpgp-02
  - draft-wouters-dane-otrfp-01

Instant Messaging

- real-time text transmission over the Internet

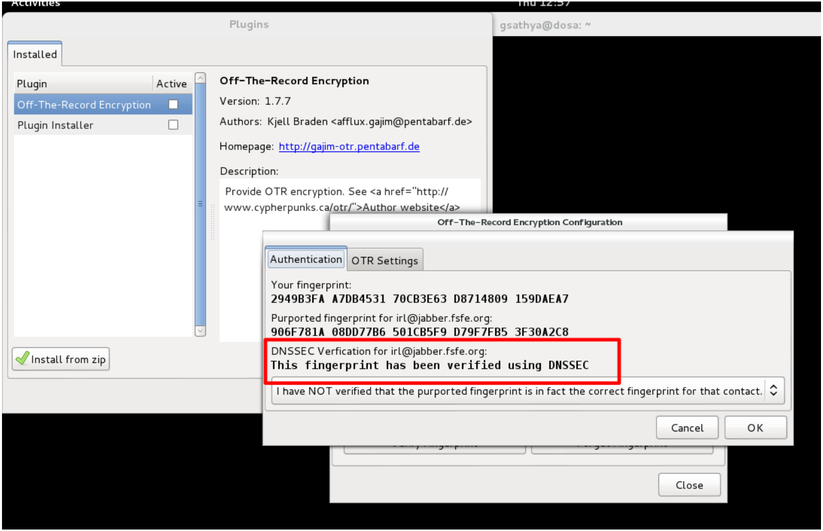
Off-The-Record

> *Off-the-Record Messaging, commonly referred to as OTR, is a cryptographic protocol that provides strong encryption for instant messaging conversations.*
>
> – Wikipedia

OTR Fingerprints

906F781A08DD77B6501CB5F9D79F7FB53F30A2C8

Verifying fingerprints with DNSSEC



Off-The-Record Encryption

Version: 1.7.7

Authors: Kjell Braden <afflux.gajim@pentabarf.de>

Homepage: http://gajim-otr.pentabarf.de

Description:

Provide OTR encryption. See <a href="http://www.cypherpunks.ca/otr/">Author website</a>

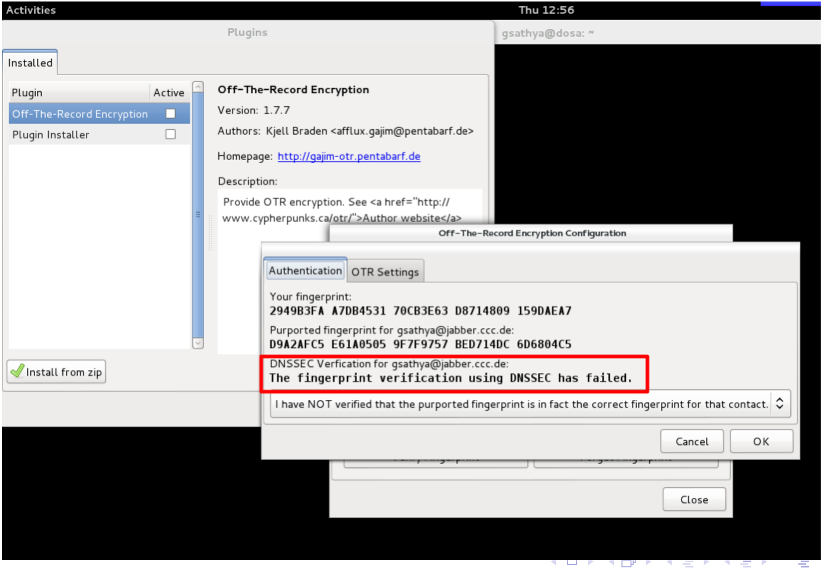
Your fingerprint:
2949B3FA A7DB4531 70CB3E63 D8714809 159DAEA7

Purported fingerprint for irl@jabber.fsfe.org:
906F781A 08DD77B6 501CB5F9 D79F7FB5 3F30A2C8

DNSSEC Verfication for irl@jabber.fsfe.org:
This fingerprint has been verified using DNSSEC

I have NOT verified that the purported fingerprint is in fact the correct fingerprint for that contact.

Verifying fingerprints with DNSSEC



Off-The-Record Encryption

Version: 1.7.7

Authors: Kjell Braden <afflux.gajim@pentabarf.de>

Homepage: http://gajim-otr.pentabarf.de

Description:

Provide OTR encryption. See <a href="http://www.cypherpunks.ca/otr/">Author website</a>

Your fingerprint:

```
2949B3FA A7DB4531 70CB3E63 D8714809 159DAEA7
```

Purported fingerprint for gsathya@jabber.ccc.de:

```
D9A2AFC5 E61A0505 9F7F9757 BED714DC 6D6804C5
```

DNSSEC Verfication for gsathya@jabber.ccc.de:

```
The fingerprint verification using DNSSEC has failed.
```

I have NOT verified that the purported fingerprint is in fact the correct fingerprint for that contact.

http://getdnsapi.net/dnskeys

The research described here is supported by the award made by the RCUK Digital Economy programme to the dot.rural Digital Economy Hub; award reference: EP/G066051/1.

The research has also received support from Versign Labs and NLNet Labs.