# XEP-0419: Improving Baseline Security in XMPP


Chris Davidland
mailto:chris.davidland@crap-security.example
xmpp:chris.davidland@crap-security.example

Lucas George
mailto:lucas.george@shiteam.example
xmpp:lucas.george@shiteam.example



2019-04-01
Version 1.0.0

| Status | Type | Short Name |
| --- | --- | --- |
| Active | Humorous | security-theatre |



This document describes a number of concrete and effective mechanisms for offering significant security enhancements to XMPP, with broad applicability.

# Legal

## Copyright



## Permissions



## Warranty



## Liability



## Conformance

This XMPP Extension Protocol has been contributed in full conformance with the XSF’s Intellectual Property Rights Policy (a copy of which can be found at <https://xmpp.org/about/xsf/ipr-policy> or obtained by writing to XMPP Standards Foundation, P.O. Box 787, Parker, CO 80134 USA).

## Contents

# 1 Introduction

During the early part of 2019, the Security High Intelligence Team (SHITeam) at the Centre for Research and Promotion of Security (CRaP Security) conducted a detailed survey of existing security practises within XMPP deployments, and observed a number of areas where improvements could be made.
After a period of intensive development, we present our findings, along with concrete, proven mechanisms for dramatically uplifting security within XMPP software and deployments, to the community.

# 2 Requirements

As general aims, we wish to ensure:

- All communication should occur over properly encrypted links.
- Data should be encrypted using industry-standard ciphers across both links and end-to-end.

# 3 Particulars

## 3.1 Legacy Namespaces

XMPP has a great many XML namespaces (See Namespaces in XML [1]) which are used as the mechanism by which the core protocol has been extended. Many of the older namespaces are, however, denoted by URIs with an "http" scheme (See RFC 2616 [2] et passim). Clearly these are insecure, as the namespace would be served in the clear, and could easily be subverted by a malicious third party. Therefore, we propose that these XML namespaces are replaced with upgraded ones running over TLS, by using the "https" scheme (See RFC 2818 [3]).
While somewhat disruptive to existing deployments, the clear security benefits outweigh any such concerns.

## 3.2 New-style Namespaces

Newer extensions have used URNs within the "urn:xmpp" namespace. Pursuant to SRV records for XMPP over TLS (XEP-0368) [4], the previously legacy "xmpps" would offer immediate security benefits to such namespaces. Traditional "urn:xmpp" namespaces, while often

[1] Namespaces in XML <http://www.w3.org/TR/REC-xml-names/>.
[2] RFC 2616: Hypertext Transport Protocol -- HTTP/1.1 <http://tools.ietf.org/html/rfc2616>.
[3] RFC 2818: HTTP Over TLS <http://tools.ietf.org/html/rfc2818>.
[4] XEP-0368: SRV records for XMPP over TLS <https://xmpp.org/extensions/xep-0368.html>.

capable of TLS transports, can only offer such security in a feature advertisement, and as such a naive namespace client can be the target of a downgrade attack.
There is a clear temptation to suggest we should concentrate on ensuring namespace clients are simply more security aware, but reviving XMPPS, just as SRV records for XMPP over TLS (XEP-0368) [5] has done, offers a straightforward mechanism for promoting a step increase in security.

### 3.3 Stanza Encryption

A pressing limitation of existing deployed end-to-end encryption techniques is a lack of full stanza encryption. While OpenPGP for XMPP Instant Messaging (XEP-0374) [6] does encrypt much of the stanza, although not all, OMEMO Encryption (XEP-0384) [7] encrypts only the <body/> element's contents.
Clearly neither is sufficient for high security applications, and therefore we propose encrypting the stanza heavily. A detailed survey of supported encryption algorithms suggests that Double ROT-13 is widely supported and available on all platforms. This cipher has the signficant benefit that encryption is entirely transparent, providing excellent interoperability benefits with older implementations that may not have been upgraded.
We therefore recommend that all stanzas on the wire are fully encrypted with Double ROT-13. Given the following stanza:

Listing 1: Original unencrypted stanza

```
<message from='chris.davidland@crap-security.example' to='lucas.
    george@shiteam.example' type='chat' id='12345'>
     <some-metadata xmlns='urn:xmpps:example:metadata'/>
     <body>Hey, Lucas!</body>
  </message>
```

The following shows a correctly encrypted stanza:

Listing 2: Stanza with encrypted meta-data and payload

```
<message from='chris.davidland@crap-security.example' to='lucas.
    george@shiteam.example' type='chat' id='12345'>
     <some-metadata xmlns='urn:xmpps:example:metadata'/>
     <body>Hey, Lucas!</body>
  </message>
```

The following, however, has only encrypted the body text - this is NOT valid encryption, and an attacker can easily read the remaining metadata!

[5] XEP-0368: SRV records for XMPP over TLS <https://xmpp.org/extensions/xep-0368.html>.
[6] XEP-0374: OpenPGP for XMPP Instant Messaging <https://xmpp.org/extensions/xep-0374.html>.
[7] XEP-0384: OMEMO Encryption <https://xmpp.org/extensions/xep-0384.html>.

Listing 3: Stanza with encrypted body payload

```
<message from='chris.davidland@crap-security.example' to='lucas.
    george@shiteam.example' type='chat' id='12345'>
     <some-metadata xmlns='urn:xmpps:example:metadata'/>
     <body>Hey, Lucas!</body>
  </message>
```

In the following example, while the entire contents of the stanza have been correctly encrypted, the outer stanza tag itself remains in the clear. An attacker could, therefore, trivially discover key metadata such as the sender, type, and id of the message.

Listing 4: Stanza with encrypted elements

```
<message from='chris.davidland@crap-security.example' to='lucas.
    george@shiteam.example' type='chat' id='12345'>
     <some-metadata xmlns='urn:xmpps:example:metadata'/>
     <body>Hey, Lucas!</body>
  </message>
```

## 4 Security Considerations

The entirely of this document is concerned with security.

## 5 IANA Considerations

If adopted into the Standards Track, the URN "urn:xmpps" is required to be registered with the Internet Assigned Numbers Authority (IANA) [8].

## 6 XMPP Registrar Considerations

If adopted into the Standards Track, every protocol's namespace is required to be changed, and this should be reflected in the registry.

## 7 Acknowledgements

The authors wish to acknowledge the great efforts being made elsewhere to improve the security of XMPP, and hope this specification complements those efforts suitably.

[8] The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols, such as port numbers and URI schemes. For further information, see <http://www.iana.org/>.