Was ist SASL ?
Simple Authentication and Security Layer

Tino Reichardt

März 2004

Gliederung

1. Begriffsklärung und Abkürzungen
2. Schichten und Protokolle
3. Standardisierung von SASL
4. Erläuterung mit Beispielen von SMTP / POP3
5. Zusammenfassung

Wofür steht SASL ?

- Englisch: Simple Authentication and Security Layer
- Sammlung von Verfahren zur Authentisierung

Was ist eine RFC ?

- Englisch: Request for Comments
- ASCII Dokumente mit Spezifikationen
- Architektur des Internets beruht darauf
- Vorschläge dür neue Protokolle und Verfahren
- für Hersteller, Programmierer, Systembetreuer und technische Spezialisten
- Beispiel: DNS ist durch diese RFC's spezifiziert: 1034, 1101, 1876, 1982 und 2065

Schichten und Protokolle

- gehört in die OSI Schichten 5-7
  - Schicht 5: Kommunikation
  - Schicht 6: Darstellung
  - Schicht 7: Anwendung

- ist für textbasierte Netzwerkprotokolle entwickelt
  z.B.: SMTP, POP3, IMAP, ACAP, LDAP, ggfs. HTTP + FTP

Wieso ein Extra Standard für Authentisierung ?

- einheitliches Verfahren zur Authentisierung in verschiedenen Protokollen möglich
- sicherheitsrelevanter Code von Servern/Clients wird verkleinert
- SASL Mechanismen sind eindeutig definiert und offen zugänglich: http://www.iana.org/assignments/sasl-mechanisms

Spezifikationen von SASL ?

- RFC 2222 Simple Authentication and Security Layer (SASL)
- RFC 1734 POP3 AUTHentication command
- RFC 1939 Post Office Protocol - Version 3
- RFC 2195 SASL Mechanism CRAM-MD5
- RFC 2595 SASL Mechanism PLAIN
- RFC 2831 SASL Mechanism DIGEST-MD5
- und zustäzliche Spezifikation von Herstellern wie Microsoft

SMTP - Simple Mail Transfer Protokoll

- läuft auf Port 25 (465)
- Authentisierung zum versenden von Mail nötig
- Server im Internet unterstützen verschiedene Methoden:
  - POP before SMTP
  - ESMTP AUTH Kommando (quasi SASL)
  - ESMTP EHLO
  - gar keine Authentisierung

Post Office Protokoll 3

- läuft auf Port 110 (995)
- Authentisierung zum empfangen von Mail nötig
- Server im Internet unterstützen verschiedene Methoden:
  - USER + PASS (RFC 1939)
  - APOP (RFC 1939)
  - AUTH Kommando (RFC 1734, quasi SASL)
  - CAPA (RFC 2449)

SMTP - Empfangen einer Mail

```
S: 220 nice to meet you
C: EHLO mail3.bluewin.ch
S: 250-nice to meet you
S: 250-AUTH LOGIN PLAIN CRAM-MD5 CRAM-SHA1 DIGEST-MD5
S: 250-ENHANCEDSTATUSCODES
S: 250-PIPELINING
S: 250-STARTTLS
S: 250-SIZE 10000000
S: 250 8BITMIME
C: MAIL FROM:<m.ostion-miri@bluewin.ch> SIZE=1559
S: 250 2.1.0 ok
C: RCPT TO:<info@wweshopzone.de>
S: 250 2.1.0 ok
C: DATA
```

```
S: 354 go ahead
C: [...] bytestooverflow=3559
S: 250 2.6.0 ok 1079104732 qp 6299
C: QUIT
S: 221 2.0.0 good bye!
```

SMTP - Empfangen einer Mail / TLS

```
S: 220 nice to meet you
C: EHLO codeblau.de
S: 250-nice to meet you
S: 250-AUTH LOGIN PLAIN CRAM-MD5 CRAM-SHA1 DIGEST-MD5
S: 250-ENHANCEDSTATUSCODES
S: 250-PIPELINING
S: 250-STARTTLS
S: 250-SIZE 10000000
S: 250 8BITMIME
C: STARTTLS
S: 220 2.7.0 ready for tls
C: EHLO codeblau.de
S: 250-nice to meet you
S: 250-AUTH LOGIN PLAIN CRAM-MD5 CRAM-SHA1 DIGEST-MD5
```

```
S: 250-ENHANCEDSTATUSCODES
S: 250-PIPELINING
S: 250-SIZE 10000000
S: 250 8BITMIME
C: MAIL FROM:<dietlibc-return-1189-list=mcmilk.de@fefe.de>
S: 250 2.1.0 ok
C: RCPT TO:<list-dietlibc@mcmilk.de>
S: 250 2.1.0 ok
C: DATA
S: 354 go ahead
C: [...] bytestooverflow=10002000
S: 250 2.6.0 ok 1079287401 qp 22926
C: QUIT
S: 221 2.0.0 good bye!
```

SMTP - Beispiel SASL LOGIN

```
S: 220 nice to meet you
C: EHLO aspire.mcmilk.de
S: 250-nice to meet you
S: 250-AUTH LOGIN PLAIN CRAM-MD5 CRAM-SHA1 DIGEST-MD5
S: 250-ENHANCEDSTATUSCODES
S: 250-PIPELINING
S: 250-STARTTLS
S: 250-SIZE 10000000
S: 250 8BITMIME
C: AUTH LOGIN
S: 334 VXNlcm5hbWU6
C: ZWJheUB3d2VzaG9wem9uZS5kZQ== (der@mcmilk.de)
S: 334 UGFzc3dvcmQ6
C: dGVzdAo= (test)
```

```
S: 235 2.0.0 auth ok, go ahad
C: MAIL FROM:<der@mcmilk.de> SIZE=1234
S: 250 2.1.0 ok
C: RCPT TO:<info@lala.de>
S: 250 2.1.0 ok
C: DATA
S: 354 go ahead
C: [...] bytestooverflow=3234
S: 250 2.6.0 ok 1079104732 qp 629
C: QUIT
S: 221 2.0.0 good bye!
```

POP3 - Post Office Protokoll 3

```
S: +OK <6609.1078954431@mail.svc-box.de>
C: USER ebay@wweshopzone.de
S: +OK
C: PASS xyz
S: +OK
C: STAT
S: +OK 1 5481
C: UIDL
S: +OK 1 messages (5481 octets)
S: [...]
C: RETR 1
S: +OK (5481 octets)
S: [...]
C: DELE 1
```

```
S: +OK
C: QUIT
S: +OK good bye
```

POP3 - SASL CRAM-MD5

```
S: +OK <21464.1079285158@mail.svc-box.de>
C: CAPA
S: +OK list of capabilities follows
S: SASL LOGIN PLAIN CRAM-MD5 CRAM-SHA1 DIGEST-MD5
S: AUTH-RESP-CODE
S: TOP
S: USER
S: UIDL
S: PIPELINING
S: RESP-CODES
S: IMPLEMENTATION qmail patched md13
S: .
C: AUTH CRAM-MD5
S: + PDIxNDY0LjEwNzkyODUxNThAbWFpbC5zdmMtYm94LmRlPg==
```

```
C: dGVzdEBtY21pbGsuZGUgOTMwNWQxZTIxNWEyNzhjMTI3MTIyNzc0
   NTI4MzM2ZTc=
S: +OK
C: LIST
S: +OK 1 messages (934 octets)
S: [...]
C: UIDL
S: +OK 1 messages (934 octets)
S: [...]
C: QUIT
S: +OK good bye
```

Zusammenfassung

- SASL ist aus den Netzwerkprotokollen nicht mehr wegzudenken
- Authentisierungsmethoden für SASL wachsen stetig
- allerdings: einige Hersteller implementieren gern eigene Verfahren
- die Stärke der Sicherheit ist recht variabel:
  man vergleiche mal PLAIN mit DIGEST-MD5

Danke für die Aufmerksamkeit!

- Fragen?
- Folien bei http://www.mcmilk.de/docs/