

Internet infrastructuur

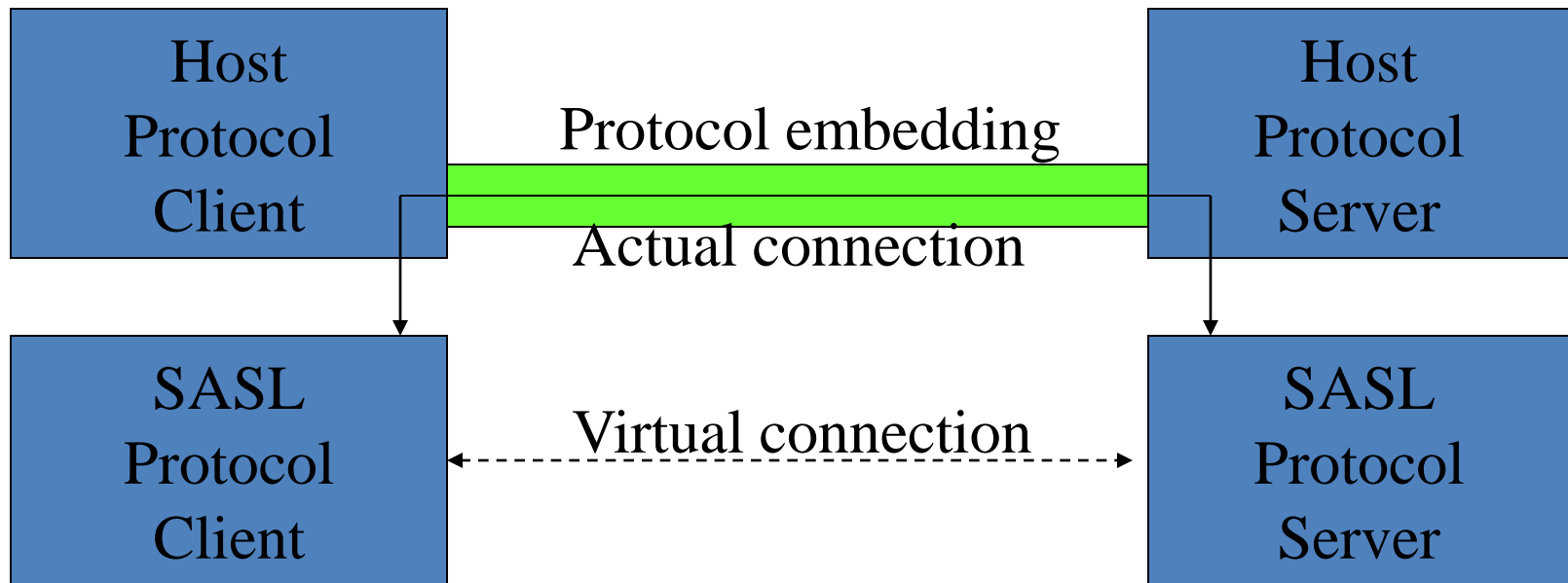
Prof. Dr. Ir. André Mariën

SASL

Simple Authentication and Security Layer

- RFC 2222: SASL
- A method for adding authentication support to connection-based protocols
- Protocol-in-a-protocol approach
- SASL could also be used to negotiate more security measures; this is not discussed here (out of scope)

SASL embedding



Scope of SASL

- Protocol to be used as a protocol-in-a-protocol
- Defines several mechanisms for use by the command
- RFC 2222: describes how to incorporate an authentication mechanism into another protocol
- RFC 2222 gives examples of protocol incorporation
- RFC 2808, RFC 2831: other mechanisms

SASL mechanism identification

- Assigned names (≤ 20 alpha-numeric)
- Registered with the IANA
- Initial:
 - EXTERNAL
 - KERBEROS_V4
 - SKEY

Authentication handshake

- Multiple messages possible
- Message data: binary tokens of arbitrary length.
- The hosting protocol's profile specifies how these binary tokens are encoded for transfer over the connection.

Example handshakes

- Server authentication:
 - Basic authentication:
 - Client: userID:password
 - Challenge/respons:
 - Server: challenge
 - Client: userID:response
- Note:
 - One-way authentication: only the server is sure
 - Man-in-the-middle: vulnerable

"KERBEROS_V4" description:

- Server: first challenge: random 32-bit number
- Client: Kerberos ticket and an authenticator for the principal "service.hostname@realm"
- Server: second challenge & response for server authentication
- Client: second response
- Server: ACK/NACK

S/Key mechanism "SKEY"

- RFC 1760
- Client: initial response with the authorization identity
- Server: a challenge: the decimal sequence number + the seed string for the indicated authorization identity
- Client: the one-time-password
- Server: ACK/NACK

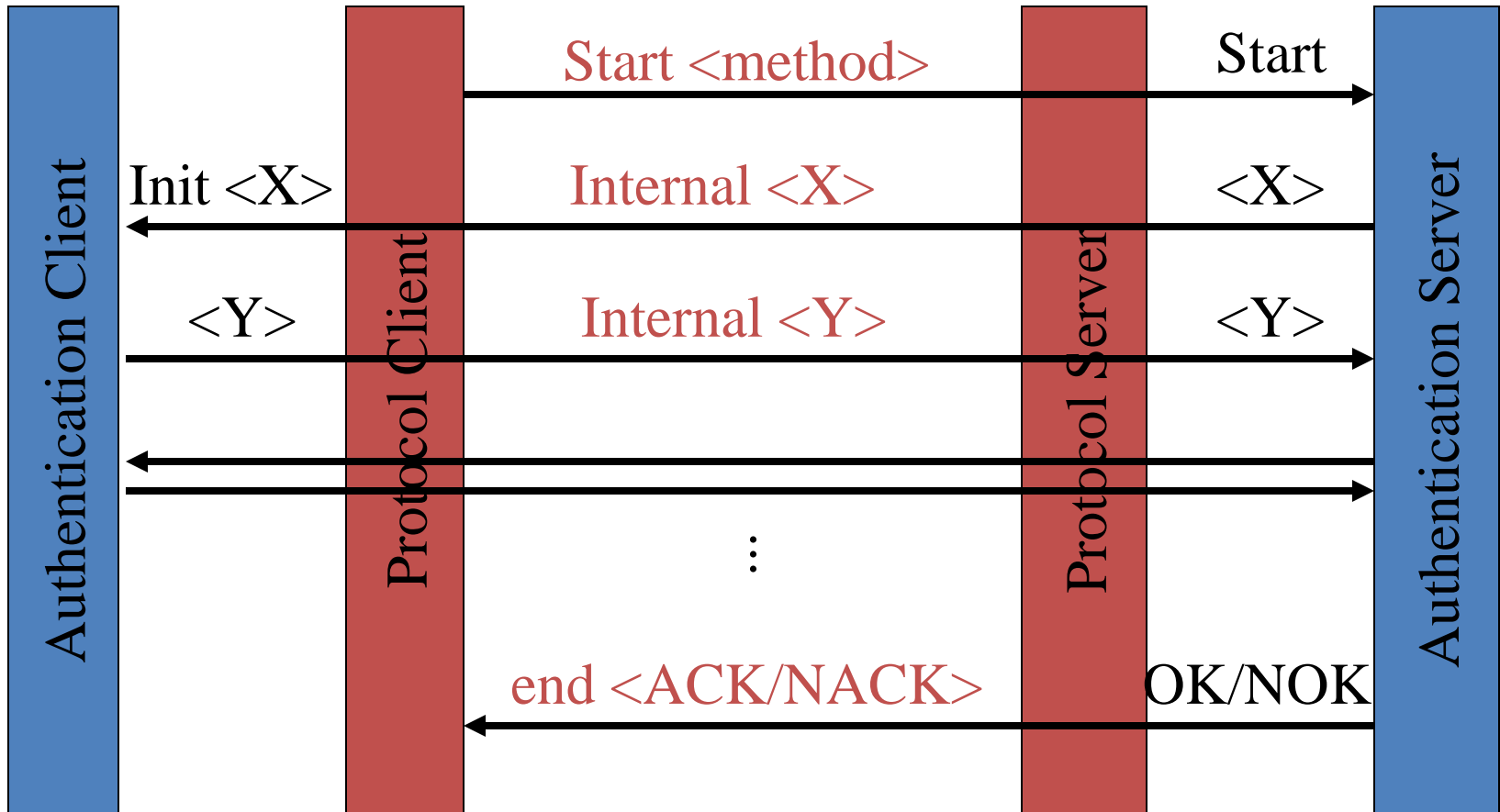
Protocol messages

- The first message is either client or server
- The number of messages is variable
- A server may send
 - a challenge
 - indicate failure
 - indicate completion
- A client may send
 - a response
 - abort the exchange.

Hosting protocol

- Defines the command to initiate the authentication protocol exchange
 - Must: command parameter: the SASL mechanism name
 - Optional: initial response
- Defines the authentication protocol exchange mechanism
 - Challenge/responses encoding
 - Server completion notification
 - Failure of the exchange

Hosting



Examples from RFC2222

- Two Kerberos version 4 login scenarios to the IMAP4 protocol
 - Successful
 - Failure

Example 1:

S: * OK IMAP4 Server

C: A001 AUTHENTICATE KERBEROS_V4

S: + AmFYig==

C: BAcAQU5EUk[...]9bpObYLGOKi1Qh

S: + or//EoAADZI=

C: DiAF5A4gA+oOIALuBkAAmw==

S: A001 OK Kerberos V4 authentication successful

Example 2:

S: * OK IMAP4 Server

C: A001 AUTHENTICATE KERBEROS_V4

S: + gcfgCA==

C: BAcAQU5EUk[...]9bpObYLGOKi1Qh

S: A001 NO Kerberos V4 authentication failed

Examples from RFC222: example 1

- S: * OK IMAP4 Server
- C: A001 AUTHENTICATE SKEY
- S: +
- C: bW9yZ2Fu
- S: + OTUgUWE1ODMwOA==
- C: Rk9VUiBNQU5OIFNPT04[...]TUFTSA==
- S: A001 OK S/Key authentication successful

Examples from RFC222: example 2:

- S: * OK IMAP4 Server
- C: A001 AUTHENTICATE SKEY
- S: +
- C: c21pdGg=
- S: + OTUgUWE1ODMwOA==
- C: BsAY3g4gBNo=
- S: A001 NO S/Key authentication failed

“EXTERNAL”

- The mechanism name associated with external authentication is "EXTERNAL".
- Client: authorization identity (or empty)
- Server:
 - check if the client is authorized to authenticate as the identity (if not empty; otherwise: authentication bridging)
 - ACK/NACK
- Example: SSL (TLS)

Responsibilities

- SASL: defines responsibilities
 - Protocol embedding: hosting protocol
 - Authentication protocols: SASL compliant definition
 - SASL Protocol name: IANA

References

- RFC 2222: Simple Authentication and Security Layer
- RFC 2554: SMTP service extension for authentication
- RFC 2808: The securID(r) SASL mechanism
- RFC 2831: using digest authentication as a SASL mechanism
 - IANA: <http://www.iana.org/assignments/sasl-mechanisms>