Some TLS ambiguities

The specification of TLS1.3 often fails to make it entirely clear what a client is supposed to do in response to information received (or not received) from the server during a protocol run.

Take for example the Server Name extension. Here the client explicitly makes clear to the server which specific URL it wants to connect with. This is clearly a good idea, particularly as some servers may be maintaining Web pages for more than one URL.

This is all handled by RFC6066 which states -

```
A server that receives a client hello containing the "server_name" extension MAY
use the information contained in the extension to guide its selection of an
appropriate certificate to return to the client, and/or other aspects of security
policy.  In this event, the server SHALL include an extension of type
"server_name" in the (extended) server hello.
```

What this means is that the server MAY respond to the client (in the “encrypted extensions” of its Server Hello) with an empty extension of type “server name”. This acts as a kind of acknowledgement to the original client request. Or the server may not respond at all – either reaction is entirely legitimate.

But what is left hanging is how is the client supposed to respond to either the reception or non-reception of such an extension? As I don’t know what to do with this information, I currently simply ignore it. But I would welcome suggestions.

Another extension along the same lines is the Application Layer Protocol Negotiation (ALPN) extension (RFC7301). This is sent by the client to the server to indicate which communications protocol it is hoping to end up engaged in, on the current TCP/IP port, after the TLS handshake has completed. The most common such protocol is of course HTTP/1.1, but many others are possible, see

https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml#alpn-protocol-ids

Again the server is supposed to respond, typically by echoing back that which the client sent. This acts as a kind of acknowledgement by the server that “I heard you”. But what to do if no such acknowledgement were received? Could be that the server simply ignored my ALPN request, or that it doesn’t implement the ALPN extension. But still I need to know what to do. Should I hang-up? Should I just hope that the server on its side has done what is necessary to ensure that I do end up in a secure HTTP session? At the moment I just print a warning to the terminal window if no acknowledgment is received, but of course in the real world no such window is open, and anyhow issuing a warning just pushes the indecision up the stack.

Does any of this matter? Well yes, apparently it does – see https://alpaca-attack.com/

The good news (for me) is that it is mainly the server’s responsibility to respond to these extensions, and it is just the clients responsibility to make sure that they are present in the initial Client Hello, (and largely ignore the presence or otherwise of a server acknowledgement). So I must just hope that the server will do the right thing.