Extensions to TLS

Simon Blake-Wilson
Certicom

David Hopwood
Independent Consultant

Jan Mikkelsen
Transactionware

Magnus Nystrom
RSA Security

Tim Wright
Vodafone

Content

- Updates from “wireless extensions”
- Issues raised
- The way forward?

DNS name extension

- New to the draft
- Allows a single “machine” to host multiple “servers”
- Client tells server DNS name of server being contacted
- Server may use info to help produce response

Other Extensions

- Clarified session resumption - extensions ignored during session resumption
- Short session IDs - removed
- Client cert urls - client supplies a list, one url = one cert
- Client cert urls - both cert hash and url supplied
- Truncated MACs - restricted to HMAC with MD5 and SHA-1
- Trusted root indication - cert hash option added

New Error Alerts

- Be careful when new error alerts get sent!

- Unsupported extension
- Bad extension order
- Unrecognized domain
- Certificate unobtainable
- Bad OCSP response

Issues

- How serious is “certificate unobtainable” alert?
- Do we need to require client driven extensions?
- How/where do DNS names get canonicalized?
- Generalize OCSP status request?
- Tie extensions with TLS version rev?

The Way Forward?

- Update based on comments and known issues
- WG last call?