DES and IDEA Cipher Suites
(draft-ietf-tls-des-idea-00)

Pasi Eronen (editor)
What?

TLS_RSA_WITH_{DES_CBC_SHA
TLS_DH_DSS_WITH_{DES_CBC_SHA
TLS_DH_RSA_WITH_{DES_CBC_SHA
TLS_DHE_DSS_WITH_{DES_CBC_SHA
TLS_DHE_RSA_WITH_{DES_CBC_SHA
TLS_DH_anon_WITH_{DES_CBC_SHA
TLS_RSA_WITH_{IDEA_CBC_SHA
Why?

- DES: key size
- IDEA: basically never used in TLS + other reasons (see next slide)
“IDEA cipher suites for TLS have not seen widespread use: most implementations either do not support them, do not enable them by default, or do not negotiate them when other algorithms (such as AES, 3DES, or RC4) are available.”
IDEA: Recommendation

“Experience has shown that rarely used code is a source of security and interoperability problems; given this, the IDEA cipher suites SHOULD NOT be implemented by TLS libraries, and SHOULD be removed from existing implementations.”
“Several reasons have been suggested to explain why the IDEA cipher suites have been rarely used. These include

• the existence of **IPR disclosures** (which can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr);

• **poor performance** in software on common CPU architectures;

• a **64-bit block size** which is considered short by modern standards;

• the existence of **weak keys**;

• **lack of government approval** in many countries; and

• the **availability of other algorithms** which addressed at least some of these reasons.”