On the Security of TLS 1.3 Against Weaknesses in PKCS#1 v1.5 Encryption

Tibor Jager, Jörg Schwenk, Juraj Somorovsky
Horst Görtz Institute for IT Security
Ruhr-University Bochum

IETF 96, Berlin
July 21, 2016
Support of TLS versions

RSA-PKCS#1 v1.5 Encryption
[RFC 2313]

• **Most widely-used** key transport mechanism in all TLS versions **before 1.3**

• **Deprecated in TLS 1.3**
  – Vulnerable: **Bleichenbacher’s attack** (CRYPTO `98)
  – Sufficient to protect against its weaknesses?
Bleichenbacher attacks over and over

• Bleichenbacher (CRYPTO 1998)
• Klima et al. (CHES 2003)
• Jager et al. (ESORICS 2012)
• Degabriele et al. (CT-RSA 2012)
• Bardou et al. (CRYPTO 2012)
• Zhang et al. (ACM CCS 2014)
• Meyer et al. (USENIX Security 2014)
• Aviram et al. (DROWN, USENIX Security 2016)

Assumption: Bleichenbacher-like attacks remain a realistic threat
Typical use of TLS 1.3 in practice
High-level Attack Description

TLS 1.3

- ClientHello
- ClientKeyShare
- ServerHello
- SKeyShare
- Certificate
- CertVerify
- S-Finished
- C-Finished

Server S

TLS 1.3

- RSA

TLS 1.0

(Backwards compatibility)

Bleichenbacher’s Attack
Practical Impact

• Typical Bleichenbacher attacks take **hours or days**

• **DROWN** [Aviram et al. 2016]:
  *forge signature in one minute* on a single CPU
  – Leverages additional vulnerability in OpenSSL
  – All OpenSSL versions from 1998 to early 2015
  – 26% of HTTPS servers were vulnerable
The difficulty of preventing such attacks (example)
The difficulty of preventing such attacks (example)

X.509 certificates do not contain protocol version!
Further difficulties

• Key separation **not supported** by major server implementations
• X.509 supports “sign/encrypt-only” certs
  – Do browsers really check this?
    • “No. And we have no intention to change this, because of usability/compatibility.”
Removing RSA-PKCS#1 v1.5 from TLS is an excellent decision
- Not sufficient to protect completely against weakness

Key separation is important
- DROWN 2.0?
- Future versions of X.509 should support key separation!
- Support by browsers is necessary!