Attacks on TLS

Douglas Stebila

Last updated June 6, 2019

Components of TLS

- RSA, DSA, ECDSA
- Diffie–Hellman, ECDH
- HMAC
- MD5, SHA1, SHA-2
- DES, 3DES, RC4, AES
- Export grade

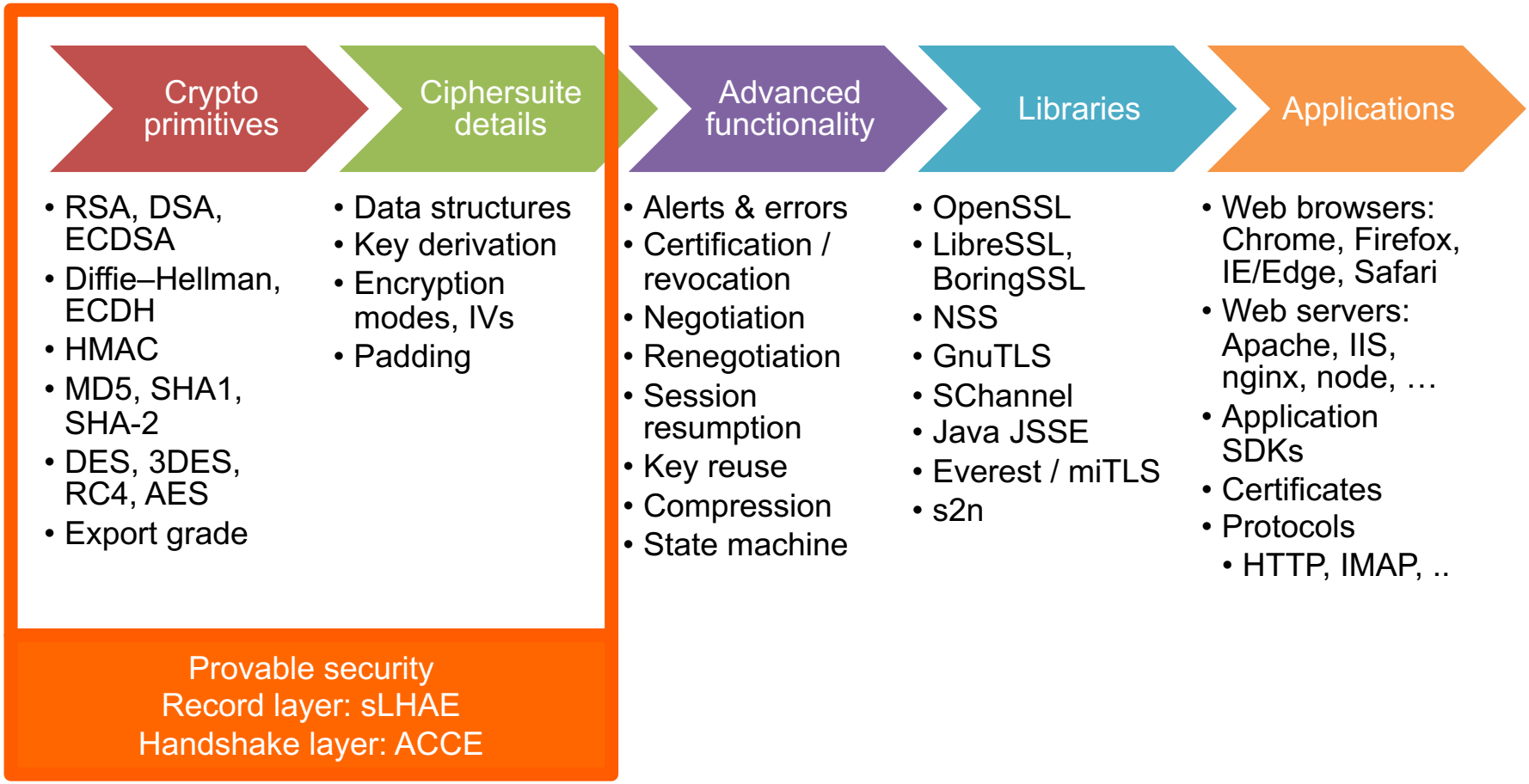
- Data structures
- Key derivation
- Encryption modes, IVs
- Padding

- Alerts & errors
- Certification / revocation
- Negotiation
- Renegotiation
- Session resumption
- Key reuse
- Compression
- State machine

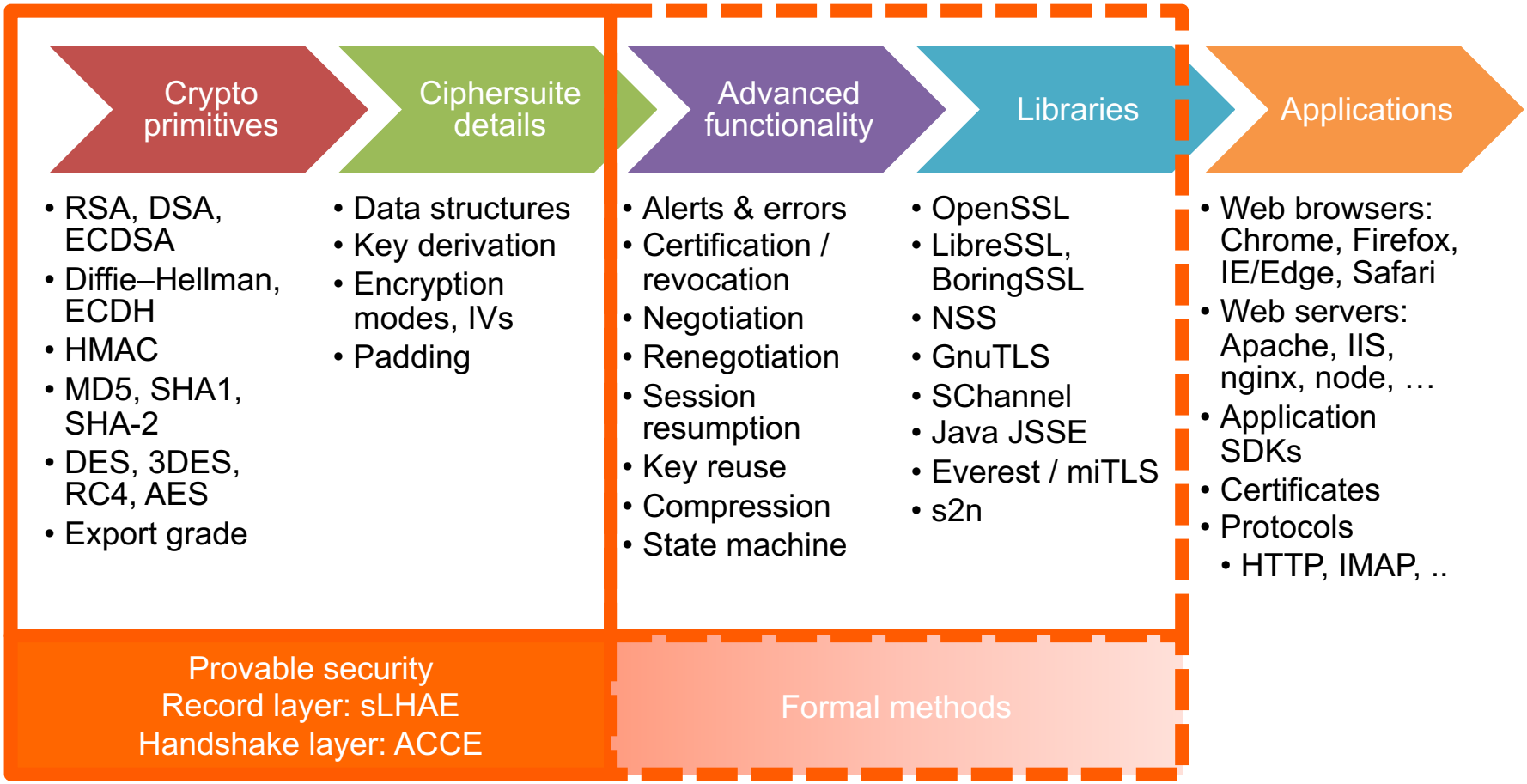
- OpenSSL
- LibreSSL, BoringSSL
- NSS
- GnuTLS
- SChannel
- Java JSSE
- Everest / miTLS
- s2n

- Web browsers: Chrome, Firefox, IE/Edge, Safari
- Web servers: Apache, IIS, nginx, node, …
- Application SDKs
- Certificates
- Protocols
  - HTTP, IMAP, ..

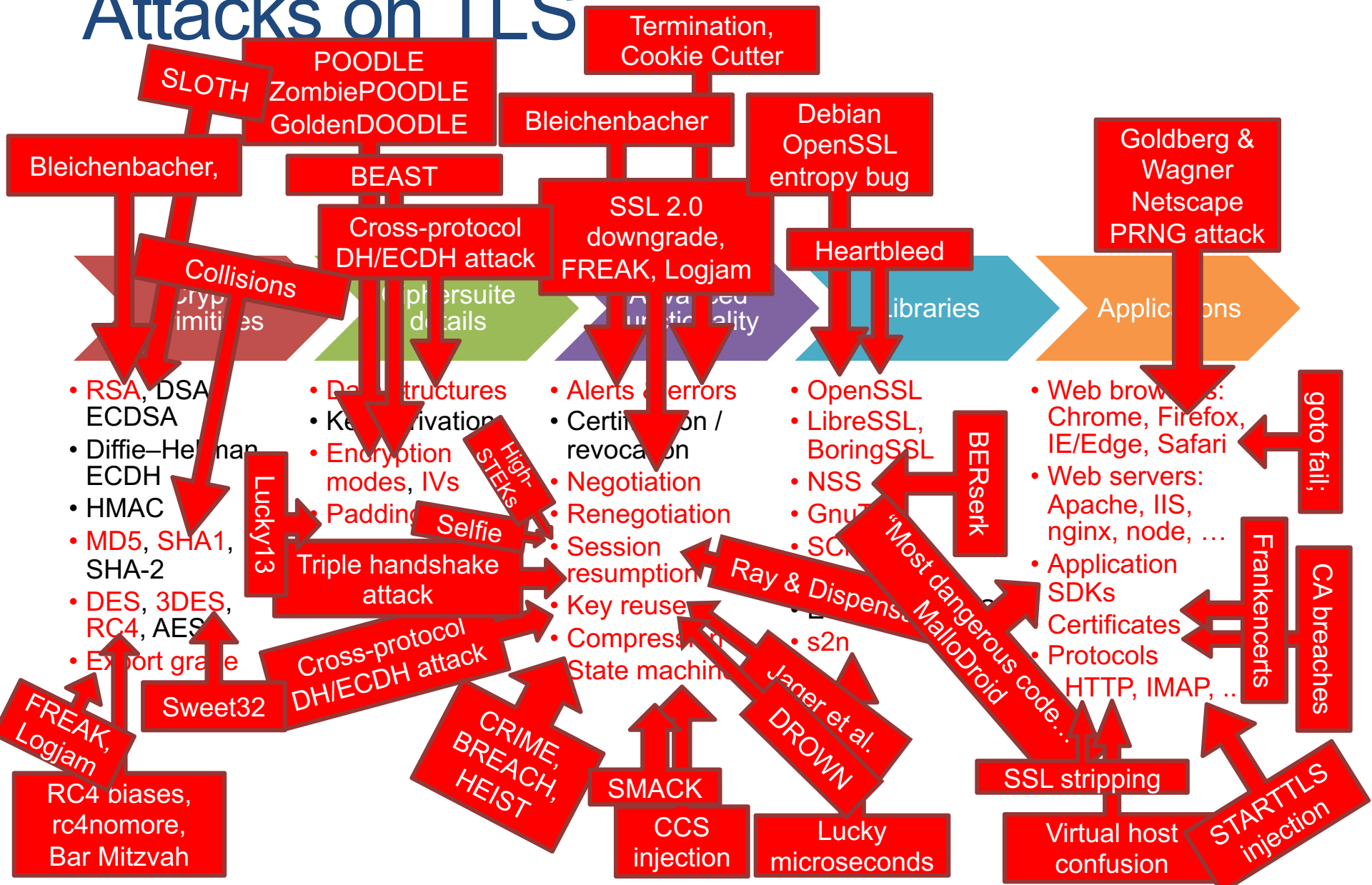
Provable security analysis of TLS



Provable security and formal methods analysis of TLS



Attacks on TLS



Attacks on TLS

Target	Attack Name	Year	Reference
Core cryptography			
RSA PKCS#1v1.5 decryption	Side channel – Bleichenbacher	1998*, 2014	[12]*, [37]
DES	Weakness – brute force	1998	[21]
MD5	Weakness – collisions	2005	[32]
RC4	Weakness – biases	2000*, 2013,15	[24, 34]*, [4, 48, 33]
RSA export keys	FREAK	2015	[8]
DH export keys	Logjam	2015	[2]
RSA-MD5 signatures	SLOTH	2016	[11]
Triple-DES	Sweet32	2011*, 2016	[44]*, [10]
Crypto usage in ciphersuites			
CBC mode encryption	BEAST	2002*, 2011	[38]*, [20]
Diffie–Hellman parameters	Cross-protocol attack	1996*, 2012	[50]*, [36]
MAC-encode-encrypt padding	Lucky 13, Lucky microseconds	2013,15	[5, 3]
CBC mode encryption + padding	POODLE, ZombiePoodle, GoldenDoodle	2014,19	[39, 52]
TLS protocol functionality			
Support for old versions	Jager et al., DROWN	2015, 2016	[27, 6]
Negotiation	Downgrade to weak crypto	1996, 2015	[50, 8, 2]
Termination	Truncation, Cookie Cutter	2007,13,14	[7, 45, 9]
Renegotiation	Renegotiation attack	2009	[42]
Compression	CRIME, BREACH, HEIST	2002*, 2012,16	[28]*, [43, 41, 47]
Session resumption	Triple-handshake attack	2014	[9]
Pre-shared keys	Selfie†	2019	[19]

* denotes theoretical basis for later practical attack

Attacks on TLS

Target	Attack Name	Year
Implementation – libraries		
OpenSSL – RSA	Side-channel	2005, 2007
Debian OpenSSL	Weak RNG	2008
OpenSSL – elliptic curve	Side-channel	2011–14
Apple – certificate validation	goto fail;	2014
OpenSSL – Heartbeat extension	Heartbleed	2014
Multiple – certificate validation	Frankencerts	2014
NSS – RSA PKCS#1v1.5 signatures	BERserk (Bleichenbacher)	2006*, 2014
Multiple – state machine	CCS injection, SMACK	2014, 2015
GnuTLS – session resumption	High-STEKs†	2020
Implementation – HTTP-based applications		
Netscape	Weak RNG	1996
Multiple – certificate validation	"Most dangerous code", MalloDroid	2012
Application-level protocols		
HTTP	SSL stripping	2009
HTTP server virtual hosts	Virtual host confusion	2014
IMAP/POP/FTP	STARTTLS command injection	2011

* denotes theoretical basis for later practical attack