@MyWebUniversity



https://

SSL · TLS · OpenSSL

Secure Your Systems

Heartbleed · patching · backup & recovery

USE TLS 1.3 · PATCH FAST



A MYWEBUNIVERSITY STORY

SSL · TLS

OpenSSL · HTTPS

Securing the Internet,
Your Systems and Data



patch · harden · backup · recover

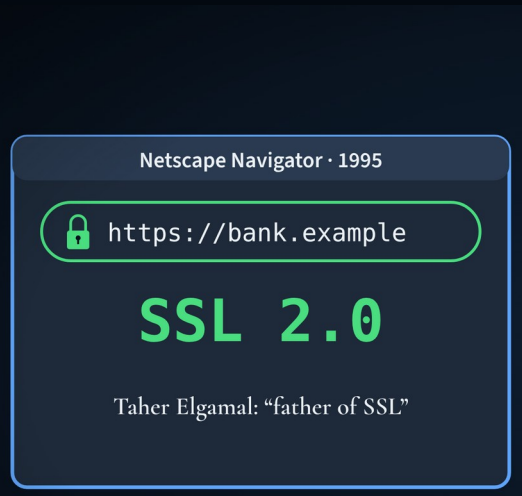
The Internet Was Like a Postcard



- Early 1990s web: everything in plain text
- Passwords and card numbers readable on the way
- E-commerce needed encryption

01

Netscape Invents SSL



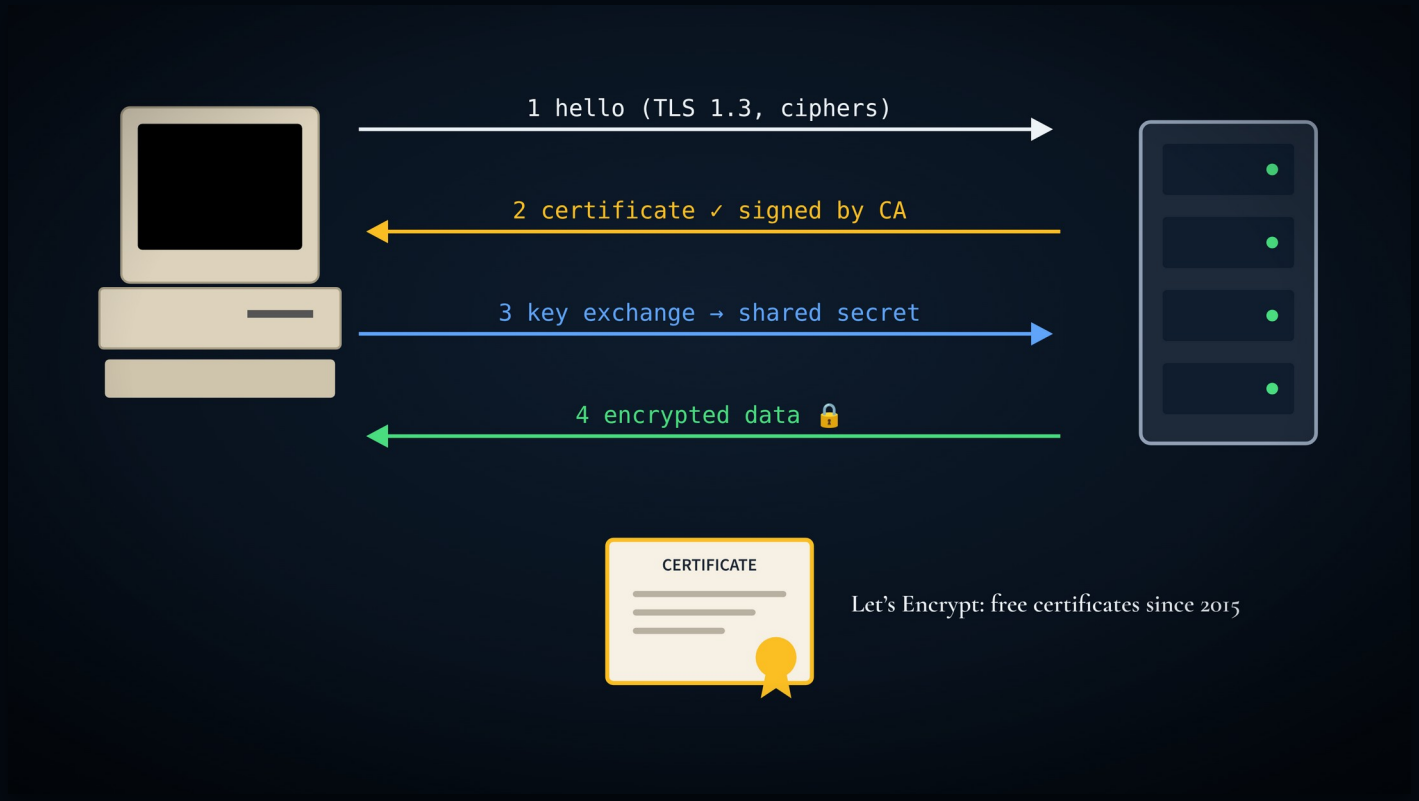
people still say “SSL” · we really use TLS

SSL 2.0	1995
SSL 3.0	1996
TLS 1.0	1999
TLS 1.2	2008
TLS 1.3	2018

- 1995: SSL 2.0, Netscape (Taher Elgamal)
- http → https and the padlock
- 1999: renamed TLS 1.0

02

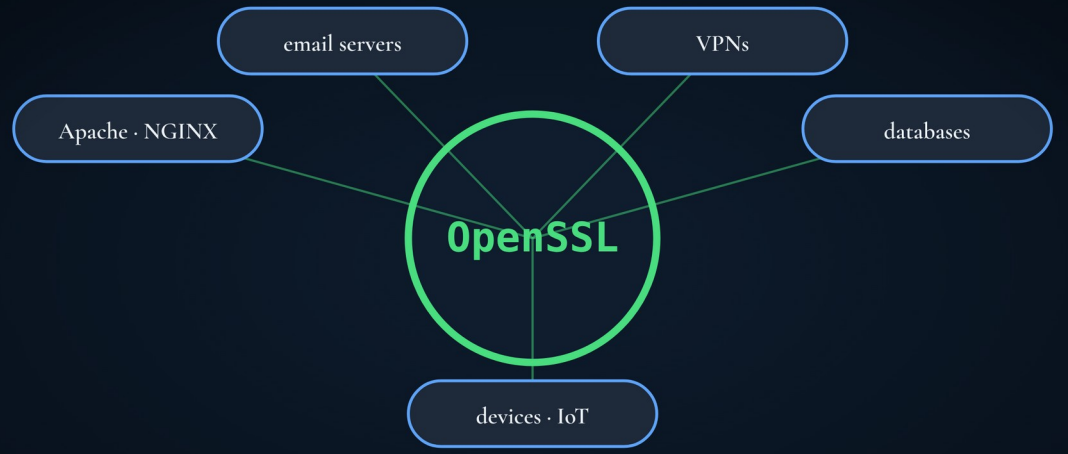
How HTTPS Works



- Certificate signed by a trusted CA
- Public-key handshake → shared secret key
- 2015+: free certificates from Let's Encrypt

03

OpenSSL



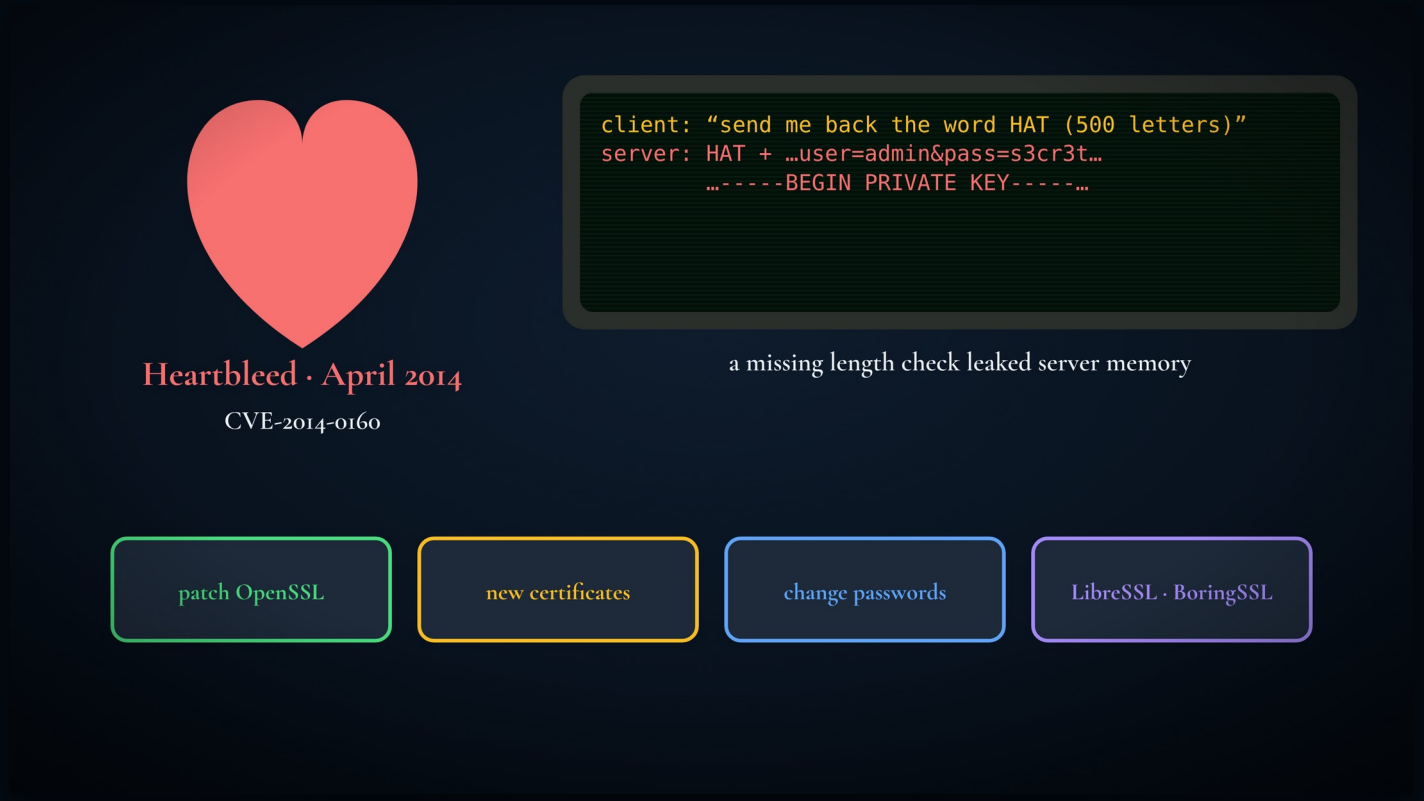
1995: Eric Young & Tim Hudson (Australia) → 1998: OpenSSL

critical software, kept alive by a few volunteers

- 1995: SSLeay (Eric Young, Tim Hudson) · 1998: OpenSSL
- Apache, NGINX, mail, VPNs, databases, devices
- Long maintained by a few volunteers

04

Heartbleed, 2014



- April 2014: Heartbleed (CVE-2014-0160)
- Missing length check leaked memory and keys
- Patch, re-issue certificates, change passwords

05

Retire Old Protocols



- Disable SSL 2/3, TLS 1.0/1.1 (POODLE, 2014)
- Use TLS 1.2 minimum
- Prefer TLS 1.3 (RFC 8446, 2018)

06

Patch Everything



- Most breaches use already-fixed CVEs
- OS (dnf/apt), DBs, web servers, Java, OpenSSL, OpenSSH, apps
- Test in staging · maintenance windows · inventory

07

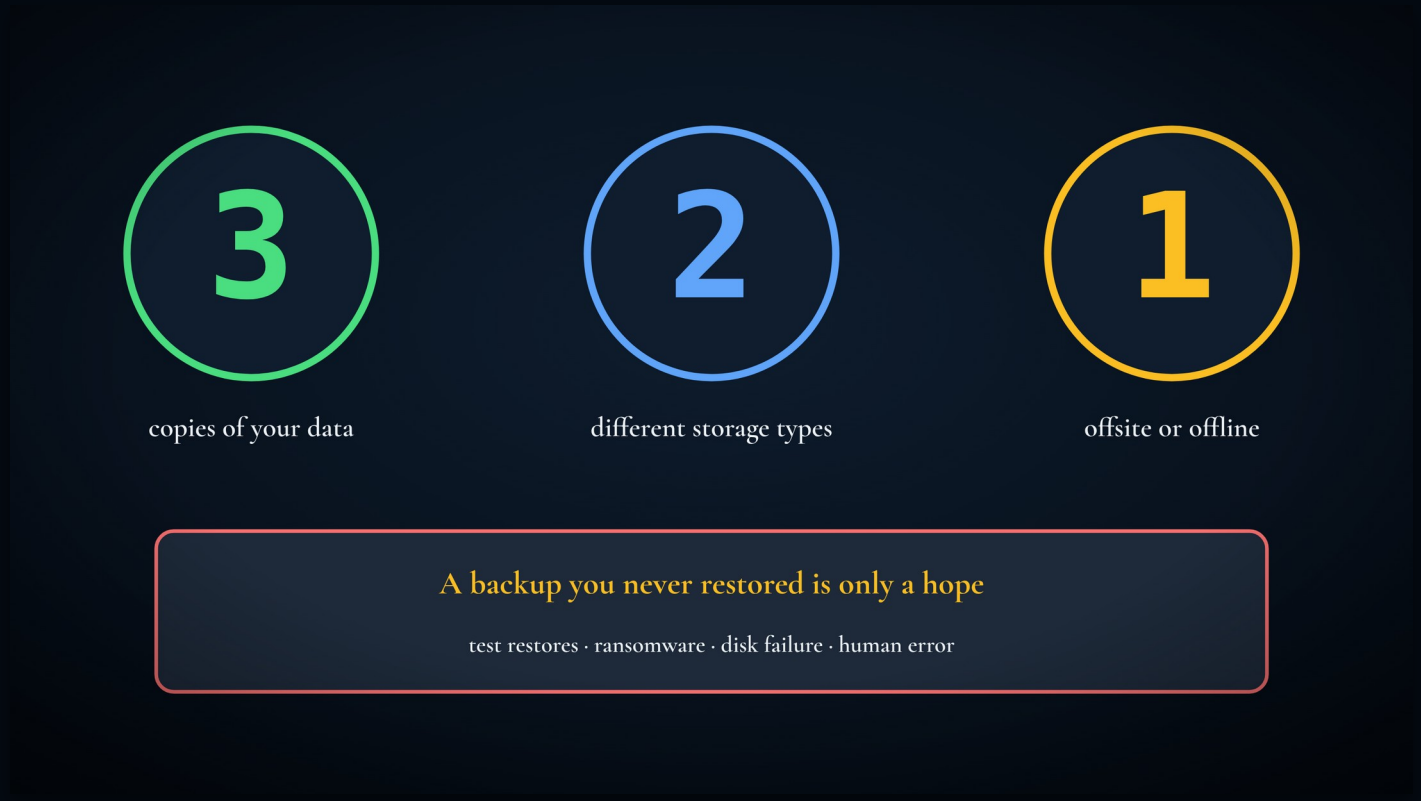
Harden the System



- Least privilege · remove unused services · firewall
- Never expose DB ports (3306, 1521) · MFA
- Encrypt in transit + at rest · watch logs

08

Backup and Recovery



- 3-2-1: 3 copies, 2 media, 1 offsite/offline
- Ransomware, failures, human error
- Test restores · know your recovery time

09

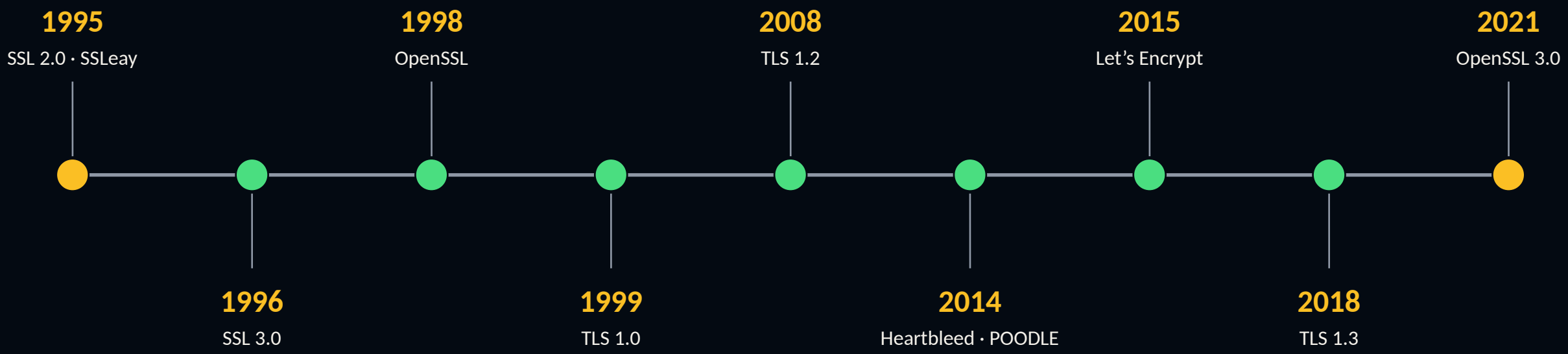
Security Is a Habit



- Security is a daily habit
- Modern TLS · fast patching · least privilege
- Watch logs · test backups

10

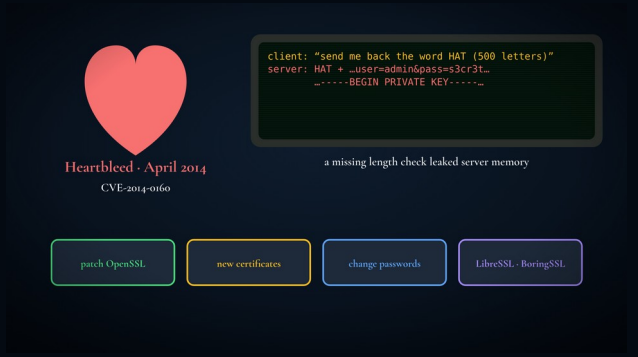
Timeline: 1995 to 2021



Sources and Further Reading

1. IETF RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3 (2018)
2. OpenSSL project history — openssl-library.org
3. Heartbleed bug (CVE-2014-0160) — heartbleed.com · NVD
4. IETF RFC 8996, Deprecating TLS 1.0 and TLS 1.1 (2021)
5. CISA, “Back Up Sensitive Business Information” (3-2-1) · Let’s Encrypt — letsencrypt.org





Thank you for watching

MyWebUniversity.com

Free technical education since 2000 — English and Dari

@MyWebUniversity · @MyWebUniversity-Dari