@MyWebUniversity-Dari

https://



SSL · TLS · OpenSSL

سیستم خود را مصئون بسازید

هارت‌بلید · پچ کردن · بکاپ و بازیابی

TLS 1.3 · سریع پچ کنید



داستانی از مای‌ویب‌یونیورسیتی

SSL · TLS

OpenSSL · HTTPS

مصئون ساختن انترنت،

سیستم‌ها و دیتای شما

patch · harden · backup · recover

https://

انترنت مثل یک کارت پستال بود

ویب اوایل دههٔ ۱۹۹۰: همه چیز متن ساده

پسورد و شمارهٔ کارت در مسیر قابل خواندن

تجارت آنلاین به رمزگذاری نیاز داشت



01

نِت‌اسکیپ اِس اِس اِل را می‌سازد

۱۹۹۵: SSL 2.0، نِت‌اسکیپ (طاهر الجمل)

https ← http و قفل براوزر

۱۹۹۹: نام نو TLS 1.0



02

اچ تی تی پی اِس چطور کار می‌کند

سرتیفیکیت امضاشده توسط CA معتبر

دست‌دادن کلید عمومی ← کلید مخفی مشترک

از ۲۰۱۵: سرتیفیکیت رایگان Let’s Encrypt



03

اوپن اِس اِس اِل

- ۱۹۹۵: SSLeay (اریک یانگ، تیم هادسن)
- ۱۹۹۸: OpenSSL

اپاچی، NGINX، ایمیل، VPN، دیتابیس، دستگاه‌ها

سال‌ها توسط چند داوطلب نگهداری شد



04

هارت‌بلید، ۲۰۱۴

اپریل ۲۰۱۴: هارت‌بلید (CVE-2014-0160)

نبود بررسی طول، حافظه و کلیدها را افشا کرد

پچ، سرتیفیکیت نو، تغییر پسوردها



05

پروتوکول‌های کهنه را کنار بگذارید

SSL 2/3 و TLS 1.0/1.1 را خاموش کنید (POODLE، ۲۰۱۴)

حداقل TLS 1.2

بهتر: TLS 1.3 (RFC 8446، ۲۰۱۸)



06

همه چیز را پچ کنید

بیشتر نفوذها از CVEهای اصلاح‌شده استفاده می‌کنند

سیستم عامل (dnf/apt)، دیتابیس، سرور وب، جاوا، OpenSSL، OpenSSH، اپ‌ها

آزمایش در staging · وقت نگهداری · فهرست نصب‌ها



07

سیستم را محکم سازید

کمترین اجازه · حذف خدمات بی‌استفاده · فایروال

پورت دیتابیس (۳۳۰۶، ۱۵۲۱) را باز نگذارید · MFA

رمزگذاری در انتقال + ذخیره · تماشای لاگ‌ها



08

بکاپ و بازیابی

۳ :۳-۲-۱ کاپی، ۲ نوع ذخیره‌ساز، ۱ بیرون/آفلاین

باج‌افزار، خرابی، اشتباه انسان

بازیابی را امتحان کنید · وقت بازیابی را بدانید



09

امنیت یک عادت است

امنیت یک عادت روزانه است

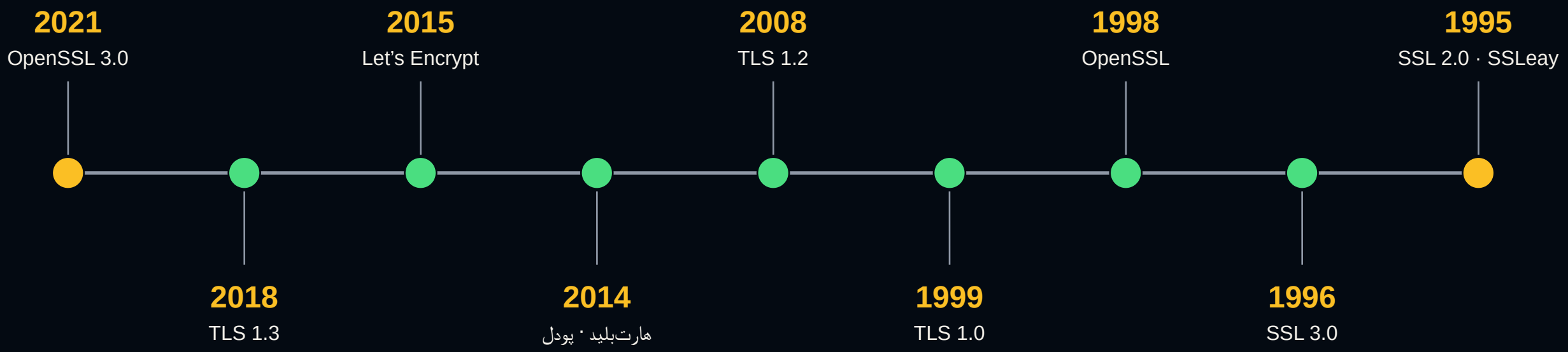
TLS مدرن · پچ سریع · کمترین اجازه

تماشای لاگ · امتحان بکاپ



10

خط زمان: 1995 تا 2021



منابع و مطالعهٔ بیشتر

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





تشکر از تماشای شما

MyWebUniversity.com

آموزش رایگان تکنالوژی از سال ۲۰۰۰ — انگلیسی و دری

@MyWebUniversity-Dari · @MyWebUniversity