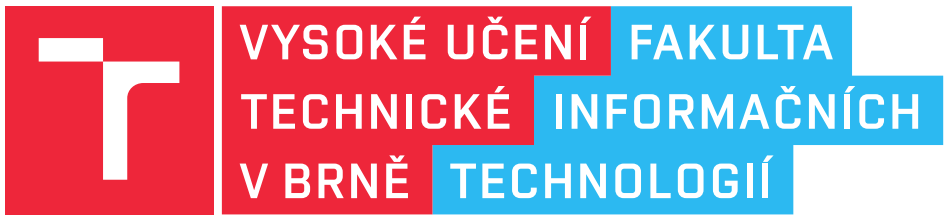
Průběžné testování interoperability knihoven TLS/SSL

František Šumšal

Vysoké Učení Technické v Brně, Fakulta Informačních Technologií
Božetěchova 1/2. 612 66 Brno - Královo Pole

xsumsa01@stud.fit.vutbr.cz



10. června 2017

Zadání

1. Seznamte se s projekty OpenSSL, NSS a GnuTLS implementující protokol SSL/TLS. Zaměřte se na testování interoperability těchto projektů.
2. Navrhněte systém pro testování interoperability a integrační testování programů a knihoven implementující SSL/TLS protokoly. Jedním z cílů systému je poskytovat testování navrhovaných změn daných projektů ještě před jejich přijetím. Systém by měl podporovat testy napsané s podporou projektu BeakerLib.
3. Implementujte systém pro testování interoperability a integračního testování. Importujte stávající testovací sady do nově implementovaného systému.
4. Kvalitu dosaženého řešení demonstrujte na příkladech s uměle vytvořenými chybami.

Testování interoperability

- Možná implementace vlastních testovacích utilit pomocí public API knihoven - zbytečné, několik verzí API, nutná údržba
- Každá knihovna poskytuje vlastní sadu utilit (openssl, gnutls-cli, selfserv, . . .)
- Využití těchto utilit v testování (velké množství přepínačů/voleb, detailní analýza komunikace, . . .)

Testovací sada

- Využit testovací framework BeakerLib (Bash)
- Původní sada testů rozšířena (rozšíření stávajících testů + implementace nových)
- Testování knihoven v párech (sady šifer, protokoly, certifikáty, . . .)

Průběžné testování (CI)

- Několik funkčních prototypů (Webhooks, Jenkins, . . .)
- Finální návrh - Travis CI (open-source, podpora GitHub repozitářů, . . .)
- Nekompatibilní OS (Ubuntu vs CentOS/Fedora) $\Longrightarrow$ Docker
- Další problémy (RHEL vs CentOS, FIPS, limity Travis CI, . . .)
- Kompilace knihovny před testováním

Výsledky

- Během vývoje a rozšiřování sady testů nalezeno několik chyb (knihovny, BeakerLib, . . .)
- Jedno CVE (CVE-2016-9574)
- Chyby ohlášeny a potvrzeny odpovědným stranám (upstream, downstream)

Budoucí vývoj

- Zdrojový kód je dostupný na GitHubu - `https://github.com/redhat-qe-security/interoperability`
- Systém průběžné integrace - `https://travis-ci.org/redhat-qe-security/interoperability`
- Naplánován další vývoj a údržba projektu
- Spolupráce s vývojáři podporovaných knihoven

Děkuji za pozornost

Otázka č. 1

Předpokládejte, že jsem autorem nové implementace TLS/SSL (nebo např. zmiňovaného BoringSSL). Jaké kroky je třeba podniknout, aby tato implementace byla podporována Vašim řešením?

- Zajistit, že je daná implementace přeložitelná na podporovaných systémech
- Rozšířit sadu testů o testy využívající danou implementaci (+CC)

Otázka č. 2

Je Vaše řešení multiplatformní? Bylo by možné testovat interoperabilitu knihoven např. na MacOS X?

- Testování probíhá v Docker kontejnerech
- Nutné přípravy (klonování repozitářů, příprava knihoven, kontrola testů, . . .)
- Na MacOS teoreticky bez úprav, na jiných systémech je třeba zajistit prvotní přípravy