Reverse Engineering (Zpětné inženýrství)

Zatímco klasické inženýrství postupuje od návrhu k výslednému produktu, zpětné inženýrství postupuje opačně. Je to klíčová disciplína v kybernetické bezpečnosti, vývoji ovladačů i v průmyslové špionáži.

1. Reverse Engineering v Softwaru

U softwaru jde o proces zkoumání binárního souboru (např. `.exe`), kterému počítač rozumí, ale člověk ne. Analytik se snaží tento kód převést do čitelnější podoby:

- **Disassembling (Zpětný překlad do assembleru):** Převod strojového kódu na instrukce procesoru (např. MOV, ADD, JMP). Výsledek vyžaduje hluboké znalosti architektury procesoru.
- **Decompilation (Dekompilace):** Pokus o automatický převod binárního kódu zpět do vyššího programovacího jazyka (např. C++ nebo Java). Výsledek je čitelnější, ale často postrádá původní názvy proměnných a komentáře.

2. Hlavní oblasti využití

Kybernetická bezpečnost

Analytici zkoumají malware, aby zjistili, co přesně dělá, kam odesílá data a jak ho zastavit. Hledají se také „zadní vrátka“ (backdoors) v softwaru.

Interoperabilita

Vývojáři zkoumají uzavřené souborové formáty nebo síťové protokoly, aby vytvořili software, který s nimi dokáže spolupracovat (např. projekt Samba pro komunikaci s Windows sítěmi).

Abandonware a opravy

Pokud firma, která software vytvořila, zanikne, je zpětné inženýrství jedinou cestou, jak opravit chyby nebo program přizpůsobit novým operačním systémům.

3. Nástroje pro Reverse Engineering

- **Disassemblery:** IDA Pro (standard v oboru), Ghidra (nástroj od NSA dostupný zdarma).
- **Debuggery:** x64dbg, OllyDbg – umožňují sledovat program „krok za krokem“ během jeho běhu.
- **Analyzátory paketů:** Wireshark – pro zkoumání síťové komunikace.

4. Právní a etické aspekty

Zpětné inženýrství je často v šedé zóně:

- **EULA:** Většina licencí placeného softwaru zpětné inženýrství výslovně zakazuje.
- **Zákon:** V mnoha zemích (včetně EU) je zpětné inženýrství legální, pokud je nezbytné pro dosažení **interoperability** (propojení s jiným programem) a pokud neexistuje jiný způsob, jak informace získat.
- **DMCA:** V USA je obcházení digitální ochrany (DRM) pomocí zpětného inženýrství často nelegální.

5. Reverse Engineering v Hardwaru

U hardwaru proces zahrnuje:

- Odstraňování pouzder čipů pomocí kyselin a jejich fotografování pod mikroskopem.
- Snímání vrstev vícevrstvých plošných spojů (PCB).
- Analýzu signálů na sběrnicích pomocí logických analytiků.

> **Zajímavost:** Jeden z nejslavnějších případů zpětného inženýrství v historii IT umožnil vznik trhu s PC klony. Firma Compaq v roce 1982 metodou „Clean Room“ (čistá místnost) zpětně analyzovala BIOS počítače IBM PC, aniž by porušila autorská práva, a vytvořila vlastní, plně kompatibilní verzi.

Zpět na Vývoj a Bezpečnost