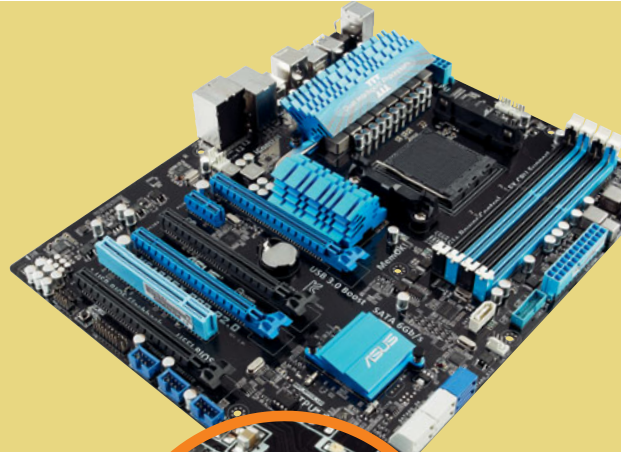


JAK SE SPOUŠTÍ UEFI

UEFI se stará o aktivaci hardwaru včetně ovladačů. Pokud je v rámci UEFI aktivována funkce Secure Boot, UEFI zkontroluje, zda mají ovladače signaturu shodnou s jeho interní databází, a vydá příkaz ke spuštění operačního systému. Pokud nedojde ke shodě podpisů, spuštění operačního systému je zastaveno. Stejnou kontrolou pravosti signatur prochází i Boot Manager a jádro instalovaného operačního systému.



AKTIVACE HARDWARU

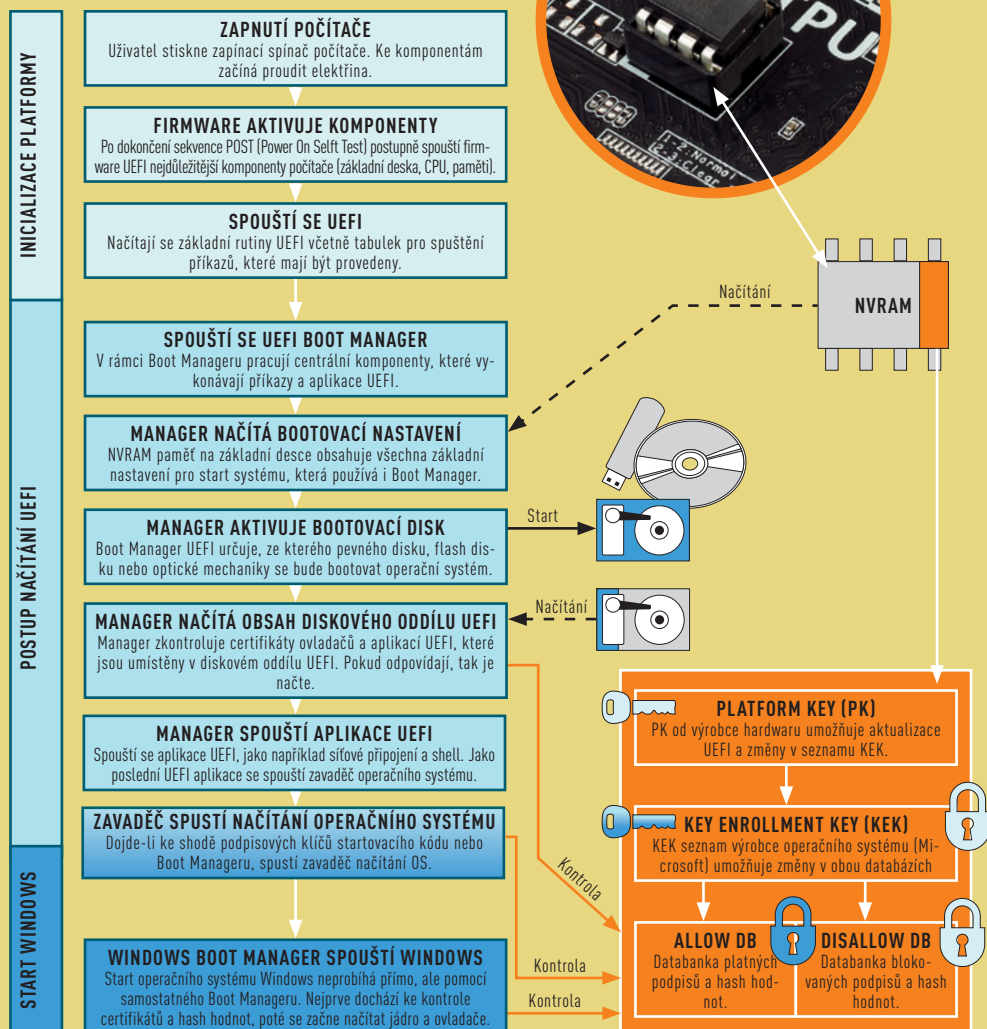
První fáze startu systémů s UEFI se nijak významně neliší od BIOS. Nejprve probíhá kontrola, zda jsou všechny hlavní součásti počítače, jako jsou deska, procesor a paměti, pod napětím, a poté se spustí aplikace UEFI.

VYVOLÁNÍ UEFI KÓDU

UEFI Boot Manager načte data aplikace UEFI z paměťového média NVRAM a z UEFI oddílu na pevném disku počítače. V tomto okamžiku také dochází ke kontrole shody signatur ovladačů a aplikace s databází podpisů Allow DB. Nakonec se spouští zavaděč operačního systému.

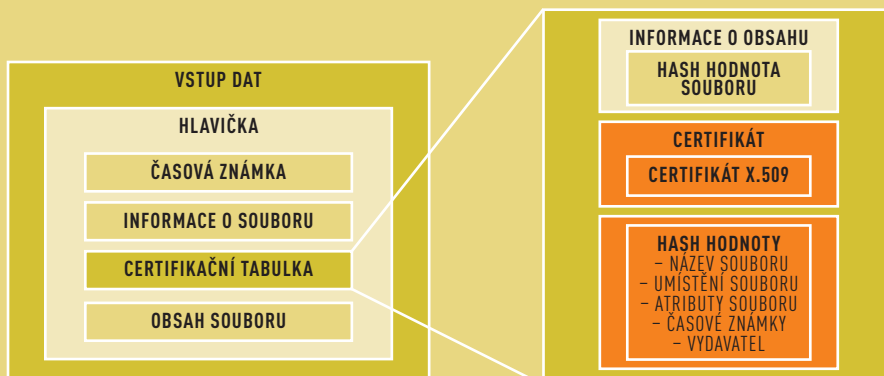
START OPERAČNÍHO SYSTÉMU

Zavaděč operačního systému startuje operační systém buď přímo, nebo prostřednictvím Boot Manageru. Startovací kód OS i Boot Manager musí mít platnou bootovací certifikaci, jinak zavaděč start systému přeruší. Stejně pravidlo platí pro všechny další komponenty jádra OS, které Boot Manager postupně načítá.



KONTROLA SECURE BOOT

Při aktivované funkci Secure Boot musí mít důležité součásti operačního systému (jádro, ovladače) odpovídající certifikát. Certifikační tabulka souborů obsahuje vhodné klíče, které splňují požadavky standardu X.509, a dále podepsané hash hodnoty nejdůležitějších vlastností souborů. Podpis i tyto hodnoty musí odpovídat odpovídajícím záznamům v databázi Allow DB.



UEFI SECURE BOOT: Příliš bezpečný start PC

Microsoft prosazuje, aby nové počítače s Windows 8 používaly místo klasického BIOS nový systém UEFI Secure Boot. Ten ale ztěžuje instalaci jiných operačních systémů.

MARKUS MANDAU

Windows jsou nejoblíbenějším operačním systémem, bohužel ale nejen u běžných uživatelů, ale také u autorů škodlivého malwaru. Červi, viry a trojské koně představují stále větší bezpečnostní rizika, která lze sice minimalizovat prostřednictvím softwarových nástrojů, pouze software ale proti nim uživatele stoprocentně neochrání. Microsoft se proto snaží zvýšit bezpečnost svého systému pomocí systému UEFI, který disponuje funkcí Secure Boot. UEFI nahrazuje zastaralý BIOS a počítače, které používají UEFI se zapnutou funkcí Secure Boot, nedovolí rootkitům vstup do operační paměti. V režimu Secure Boot totiž UEFI spouští pouze podepsané kódy, jejichž původ ověřuje pomocí šifrované databanky. Pokud chtějí výrobci prodávat stolní počítače, tablety nebo notebooky s nálepkou „Certifikováno pro Windows 8“, musí být vybaveny UEFI s aktivovaným režimem Secure Boot.


UEFI Secure Boot sice přináší bezpečnou ochranu proti rootkitům, má ale i své nevýhody. Pokud totiž mají počítače pracovat pouze s certifikovaným kódem, ohrožuje to samé základy konceptu PC jakožto otevřené platformy, která nabízí uživatelům svobodu ve formě volby operačních systémů. Značnou a pochopitelnou nevoli tento krok vzbudil jak u příznivců systému Linux, tak i u uživatelů Windows, kteří by si rádi pořídili nový počítač, ale místo nových Windows 8 chtějí stále pracovat se staršími verzemi Windows 7 nebo XP. V případě, že je na počítači s UEFI aktivován Secure Boot, nelze na něj nahrát starší operační systém a počítač není možné ani spustit. Podívejme se podrobněji na technologii funkce Secure Boot a vysvětleme si, proč tomu tak je.

UEFI zajistí pohodlnější a rychlejší start

Unified Extensible Firmware Interface, zkráceně UEFI, má nahradit stávající systém BIOS, který slouží jako rozhraní mezi hardwarem a operačním systémem a stará se o start počítače. Ve všech nových počítačích s Windows 8 je BIOS nahrazen novějším systémem UEFI, který odstraňuje některá přežitá omezení třicet let starého konceptu BIOS. UEFI například podporuje 64bitové příkazy, umožňuje používat uživatelské rozhraní s vysokým rozlišením, které lze nově ovládat myší a pomocí dotykové obrazovky. Aplikace UEFI je uložena v nevolativním paměťovém modulu (NVRAM) nebo na pevném disku počítače. Proto si také UEFI rezervuje na pevném disku vlastní oddíl o velikosti až 200 MB. Po spuštění počítače spustí UEFI Boot Manager zavaděč operačního systému, který se stará o načtení operačního systému.

Secure Boot kontroluje systémové komponenty

V tomto okamžiku přichází do hry funkce Secure Boot, která rozhoduje o tom, zda dojde, nebo nedojde k zavedení operačního systému. Secure Boot obsahuje tři vrstvy šifrování. Na nejvyšší úrovni se nachází tzv. „Platform Key“ (PK), který je vytvořen výrobcem hardwaru. PK se stará o aktualizace firmwaru UEFI a spouštění nových klíčů „Key Enrollment Keys“ (KEK). Podle definovaného standardu UEFI musí KEK klíče pocházet od vývojářů různých operačních systémů, realita je ale bohužel jiná. V praxi mají dosud všechny počítače integrován pouze KEK od Microsoftu, určený pro Windows 8. S jedinou výjimkou notebooku Google Chromebook jsou bohužel zatím všechny počítače obsahující UEFI s funkcí Secure Boot dodávány se systémem Windows 8. KEK zastávají v rámci Secure Boot klíčovou roli, protože obsahují dva klíče, které odemkají databázi s povolenými podpisy (Allow DB) a databázi s nepovolenými podpisy (Disallow DB). Pouze KEK mohou měnit údaje v těchto databázích. V seznamu Allow DB se nachází jak signatury aplikace UEFI, tak podpisy a/nebo hash hodnoty částí operačního systému, jako jsou například Boot Manager, jádro a ovladače. Systém UEFI povolí spuštění počítače pouze v případě, že jsou tyto podpisy k dispozici. Pokud nejsou, uživatel uvidí na obrazovce hlášení „Secure Boot Violation“ a operační systém se nenačte.

Secure Boot pracuje v kombinaci s Windows 8 bez problémů, Microsoft však nedodává signatury pro starší operační systémy, jako jsou Windows 7 nebo Windows XP. Počítače dodávané s linuxovými distribucemi musí mít od výrobce funkci Secure Boot deaktivovanou. Pro Linux zatím existuje pouze podepsaný boot loader Shim a loader pro Linux Foundation. Oba se načítají ještě před spuštěním Linux Boot Manageru (například Grub). Žádné jiné linuxové komponenty nejsou pomocí Boot Secure chráněny, protože s boot loaderem spolupracují na základě společných integrovaných signatur. Vývojáři Linuxu myšlenku Secure Boot neodmítají, už proto, že v současné době má Microsoft díky Secure Boot v rámci vývoje nových PC tak silné monopolní postavení, jaké v této doposud otevřené platformě historicky nikdy neměl. V certifikačních směrnících pro Windows 8 Microsoft výslovně uvádí, že uživatel musí mít možnost Secure Boot vypnout. Co se ale stane, pokud Microsoft tuto větu u příštího operačního systému zapomene uvést? 

AUTOR@CHIP.CZ