

Důkazy s nulovou znalostí

aneb jak prokázat svou identitu a nic při tom nevyzradit

Autentizace je proces mezi Dokazovatelem (nejčastěji uživatelem) a Ověřovatelem (například informačním systémem), při kterém Ověřovatel ověřuje, zda Dokazovatel má identitu, kterou prohlašuje. Autentizace vždy spočívá v důkazu, že Dokazovatel je držitelem určitého předmětu (např.: občanského průkazu, kryptografického tokenu), informace (např.: hesla, klíče) nebo biometrické vlastnosti (např.: otisku prstu, obrazu sítnice), o které Ověřovatel ví, že je bezpečně spojena s dokazovanou identitou.

V příspěvku se zaměříme na případ, kdy je Dokazovatel držitelem tajné informace (tajemství) a bude nás zajímat, jaká znalost o tajemství během autentizace uniká. V ideálním případě samozřejmě o tajemství neuniká informace žádná, takové autentizační metody existují a říká se jim důkazy s nulovou znalostí. Za jejich protiklad můžeme považovat metody, které zcela otevřeně vyzradí tajemství již během jedné autentizace, jako například častá autentizační metoda založená na prostém sdělení hesla. Běžně používané autentizační metody založené na symetrické nebo asymetrické kryptografii leží někde mezi těmito extrémními případy, své tajemství přímo nesdělují a ani ho při autentizaci nepoužívají způsobem, který má vlastnost důkazu s nulovou znalostí.

V příspěvku bude přiblížena základní myšlenka důkazů s nulovou znalostí, bude vysvětlen způsob, kterým se o autentizační metodě dokazuje, že je důkazem s nulovou znalostí, budou představeny příklady důkazů s nulovou znalostí a na závěr se podíváme, kde se tyto metody mohou využívat.