Certificate Pinning

Certificate Pinning je technika, která brání útokům typu **Man-in-the-Middle (MITM)**. V běžném modelu důvěry může útočník, který ovládne nebo zkompromituje některou z mnoha uznávaných certifikačních autorit, vydat falešný certifikát pro vaši doménu. Prohlížeč nebo aplikace ho pak přijme jako pravý. Pinning toto riziko eliminuje tím, že do aplikace pevně „zadrátuje“ identitu očekávaného certifikátu.

Tato metoda se nejčastěji používá v bankovních aplikacích, u sociálních sítí nebo v systémech pro přenos vysoce citlivých dat.

Jak Certificate Pinning funguje?

Při navazování spojení (TLS Handshake) probíhá standardní ověření, ke kterému se přidává krok navíc:

```
1. **Připojení:** Aplikace se připojí k serveru.
2. **Obdržení certifikátu:** Server pošle svůj certifikát.
3. **Kontrola pinu:** Aplikace porovná otisk (hash) obdrženého certifikátu (nebo jeho veřejného klíče) s otiskem, který má v sobě uložený (připnutý).
4. **Rozhodnutí:** Pokud se otisky shodují, spojení je navázáno. Pokud ne, aplikace spojení okamžitě ukončí, i kdyby byl certifikát podepsán autoritou, které telefon jinak věří.
```

Co lze "připínat" (Pinning Targets)

Vývojáři mají na výběr, co přesně budou v aplikaci kontrolovat:

Typ	Popis	Výhody/Nevýhody
Certificate Pinning	Připne se celý certifikát serveru.	Nejbezpečnější, ale při každé obnově certifikátu (např. jednou ročně) se musí aktualizovat i celá aplikace.
Public Key Pinning	Připne se pouze veřejný klíč.	Flexibilnější – klíč může zůstat stejný i při vypršení certifikátu a jeho obnově.
Root/Intermediate CA Pinning	Připne se certifikát autority, která vás podepisuje.	Méně bezpečné (stále věříte dané autoritě), ale méně údržby.

Proč je to důležité?

Hlavním cílem je eliminovat útoky, kdy se někdo vmezeří mezi vás a server:

- **Zkompromitovaná CA:** Útočník donutí autoritu vydat certifikát pro „mojebanka.cz“.
- **Podvržený kořenový certifikát:** Útočník (nebo administrátor firemní sítě) nainstaluje do vašeho zařízení svůj vlastní certifikát, aby mohl dešifrovat vaši komunikaci pro účely inspekce.

Rizika a nevýhody

Ačkoliv Pinning zvyšuje bezpečnost, přináší i značná rizika:

- **Zablokování aplikace (Brickability):** Pokud serveru vyprší certifikát nebo je nutné ho náhle vyměnit (např. z důvodu úniku klíče) a aplikace nemá v sobě „připnutý“ ten nový, všichni uživatelé se přestanou ke službě připojovat, dokud si nenainstalují aktualizaci aplikace.
- **Složitost údržby:** Vyžaduje perfektní synchronizaci mezi týmem pro správu serverů a vývojáři aplikací.
- **HPP (HTTP Public Key Pinning):** Tato technologie pro webové prohlížeče byla v roce 2018 odstraněna (v Chrome/Firefox) právě kvůli riziku, že si majitelé webů špatným nastavením trvale znepřístupní své stránky.

Související pojmy: SSL/TLS, CA (Certifikační autorita), Man-in-the-Middle, Šifrování, HTTPS, Hashování.