Zvýšení bezpečnosti PKI pomocí technologie blockchain

Pro bezpečnost klasického modelu Public Key Infrastructure (PKI) jsou klíčové důvěryhodnost certifikační autority (CA) a použitá kryptografická primitiva. PKI je velmi rozšířenou technologií využívající centralizované architektury. To s sebou však zároveň přináší zvýšené riziko napadení a zneužití CA za účelem vydání certifikátů neoprávněným entitám. Současné modely PKI nejsou odolné především vůči split-world útokům. Problémy s podvrženou identitou CA může vyřešit aplikace revoluční technologie blockchain.

bezpečnost blockchain Certificate Transparency CertLedger PKI

Public Key Infrastructure

Public Key Infrastructure (PKI) je velmi populární technologie[1], která umožňuje provádět autentizaci osob a zařízení v internetovém prostředí pomocí digitálních certifikátů vydávaných podle standardu X.509 [1, 2]. Pomocí PKI je možné provádět identifikaci komunikujících stran a vytvářet bezpečné TLS relace mezi entitami [1, 3].

Vzhledem k tomu, že se jedná o centralizovaný model řízení bezpečnosti, vystupuje jako hlavní stavební prvek daného systému důvěryhodná certifikační autorita CA (Certificate Authority, resp. Certification Authority). CA ověřuje platnost identit entit a potvrzuje validační proces vydáním digitálního certifikátu vázaného na konkrétní subjekt [3]. Jedná se o proces, během něhož je veřejný klíč (Public Key) žadatele, který je kryptograficky propojen s jeho identitou [1], podepsán soukromým klíčem certifikační autority (CA Private Key).

Za kritické místo daného přístupu lze považovat absolutní závislost garance důvěryhodnosti celého PKI systému na spolehlivosti CA [1, 2]. V případě napadení CA a zneužití jejího soukromého klíče může dojít k vydání certifikátů nelegitimním subjektům, které se budou následně schopny vydávat za legitimní entitu, a tím zneužívat důvěru ostatních klientů v CA, která příslušný certifikát vydala [1, 2, 4].

V dnešní době je populární model řešení bezpečnosti Zero Trust. Zjednodušeně ho lze charakterizovat větou: „Za žádných okolností nikomu a nikdy nedůvěřuj." Z tohoto pohledu tvoří závislost infrastruktury PKI na centrálním prvku jen těžko akceptovatelné bezpečnostní riziko. V roce 2013 bylo prezentováno několik nových modelů PKI, jejichž cílem bylo snížit počet požadavků na úroveň důvěryhodnosti CA. Jedním z řešení usilujících o vylepšení a dopracování klasického PKI modelu byla technika Certificate Transparency (CT) vyvinutá společností Google. Hlavním přínosem této technologie byla možnost detekce neoprávněně vydaných certifikátů. V praxi se však záhy ukázalo, že žádný z navržených způsobů ochrany není odolný vůči split-world útokům [1, 2, 5, 6]. V současné době je za nejmodernější řešení daného problému považována technologie blockchain. Právě ta může být velmi efektivně aplikována k zvýšení bezpečnosti modelu PKI.

Ještě než definitivně přeneseme svoji pozornost na problematiku zvýšení bezpečnosti PKI pomocí revoluční datové struktury typu blockchain, nebude od věci přiblížit si prin-

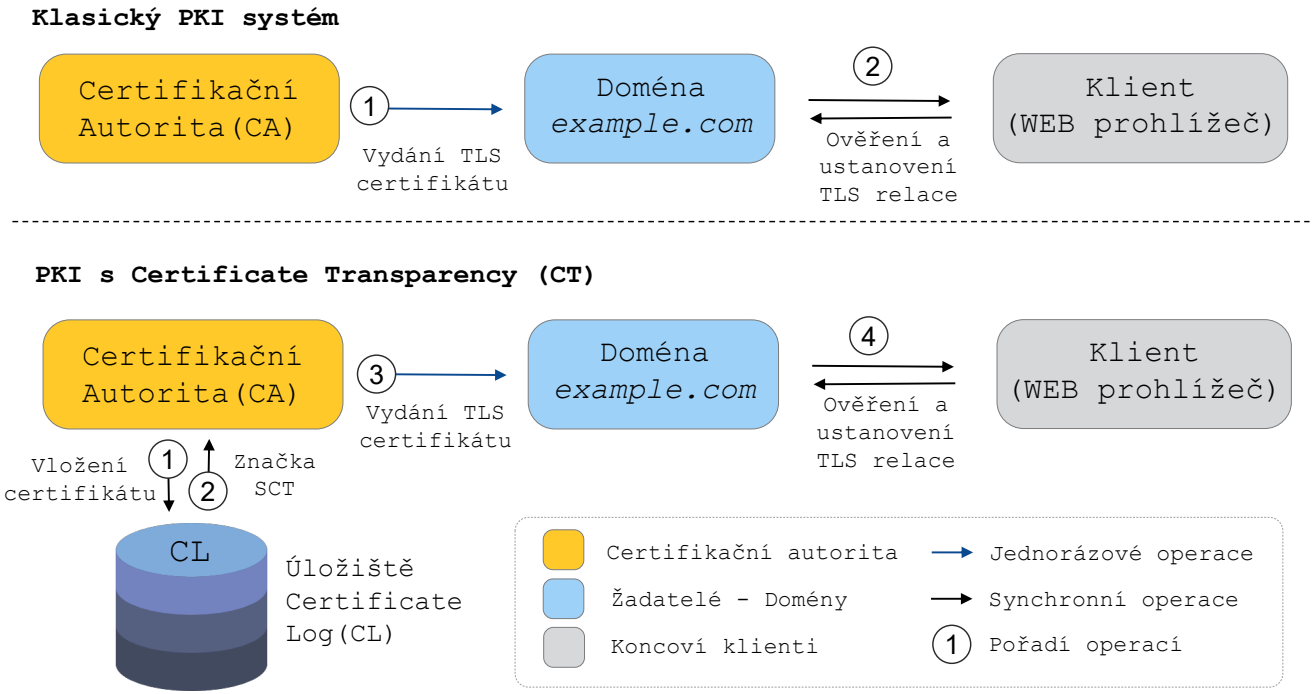
[1] O infrastruktuře veřejných klíčů je možné se podrobněji dočíst v článku „PKI v systému pro správu kryptografických klíčů", DSM 4/2019.

cip fungování technologie Certificate Transparency (CT). Společnost Google, která má v současné době dominantní vliv na prostředí WWW, už od roku 2018 ve svém prohlížeči Google Chrome použití CT [2] vynucuje. To je také jeden z důvodů, proč moderní techniky integrace PKI s blockchain staví na principech fungování CT [1, 2] anebo z nich částečně vycházejí.

Pokud rozšíříme klasický PKI model o Certificate Transparency, získáme k dispozici veřejně dostupné úložiště logů, které uchovává informace o všech vydaných CA certifikátech [7, 8]. Do základních vlastností logového úložiště lze zahrnout jeho veřejnou auditovatelnost, nemožnost odstranění záznamů nebo provedení jejich změny (charakter append only), zapojení kryptografických primitiv s důrazem na zajištění integrity, nepopiratelnosti a dostupnosti [1, 2, 7, 8].

V samotném základu Certificate Transparency leží Merkle Hash Tree (MHT). Ten klientům umožňuje ověřovat v logaritmickém čase integritu dynamické datové struktury a provádět efektivní validaci vydaných TLS certifikátů [8, 9]. MHT je možné zjednodušeně popsat jako binární strom, který uspořádává hašové otisky všech vydaných digitálních certifikátů do hierarchické struktury [1, 7, 8]. Tato datová struktura je ukončena kořenem stromu, tzv. Merkle Hash Root (MHR), jehož aktualizace se provádí při jakékoli změně dat ve struktuře stromu [1, 2, 8].

Certificate Transparency vnáší do systému PKI tři nové entity: Certificate Logs (CL), Certificate Monitors (CM) a Certificate Auditors (viz obr. 1) [1, 8]. Během procesu vydání certifikátu autorita tento certifikát distribuuje do několika entit CL, které pomocí asymetrických kryptografických primitiv vytvoří tzv. důkaz existence certifikátu v čase neboli Signed Certificate Timestamp (SCT). Zároveň s tím jsou



Obr. 1: Srovnání modelu PKI s řešením CT [8]

aktualizovány logové záznamy v MHT o ověřeném certifikátu s SCT [1]. Z technického hlediska znamená aktualizace přepočet všech hašových otisků (včetně MHR) ve větvi stromu, do které byl certifikát přidán [1, 2, 9]. V budoucnu se SCT značka certifikátu může posílat ověřovací straně jak během navázání TLS spojení, tak i v rámci rozšíření certifikátu X.509 nebo OCSP odpovědi [1].

Další entitou vyskytující se v modelu CT je Certificate Monitor. CM odpovídá za ověření veřejného logu za účelem odhalení validních, ale neoprávněně vydaných certifikátů [8]. Do množiny CM mohou spadat jak vlastníci domén, tak i soukromé organizace. Poslední množina Certificate Auditors je zastoupena ověřovateli (prohlížeči, TLS klienty apod.), kteří kontrolují validnost certifikátů spolu s SCT a také konzistenci MHT stromu [8]. V případě, kdy jedna z entit CT detekuje nelegitimně vydaný certifikát, spustí proces revokace, který se promítne do Certificate Logs a bude sdílen mezi všemi stranami modelu PKI [8].

Mezi hlavní nevýhody modelu PKI s CT patří minimální odolnost tohoto řešení vůči split-world útokům. Pokud útočník získá kontrolu nad entitami CA a Log Server [1, 2, 5, 6], může poskytovat zkreslené podoby MHT, což mu umožní snadno oklamat ověřovací stranu během procesu validace certifikátu. Další nevýhoda je definována plnou závislostí

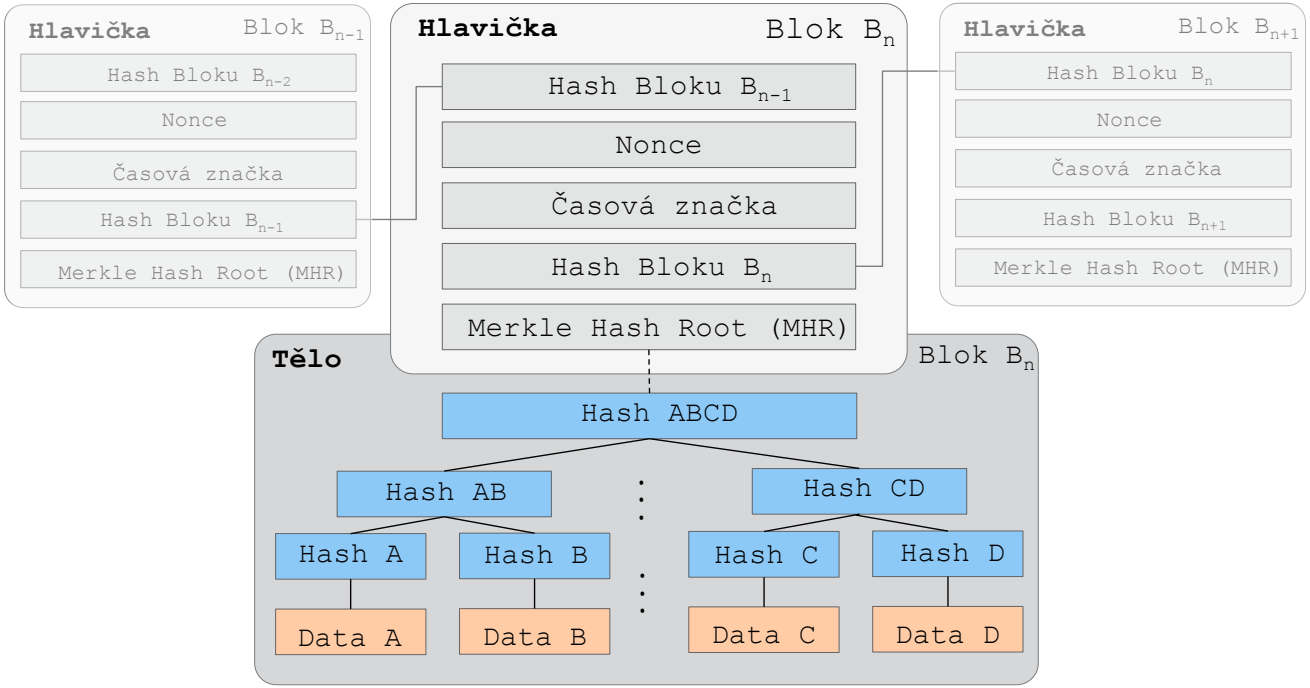
procesu revokace certifikátů a distribuce důvěryhodných klíčů na CA, která může být v reálném světě velice snadno napadena [4].

Blockchain

Technologii blockchain je možné považovat za průlomovou. Umožnila změnit představu moderní společnosti o způsobu zajištění integrity ukládání dat v nedůvěryhodném prostředí bez nutnosti zapojení třetí důvěryhodné strany [1, 2, 10, 11]. Tato technologie získala svoji popularitu především díky vzniku elektronické měny bitcoin v roce 2009. Bitcoin představuje decentralizovanou elektronickou měnu a transakční síť, která není regulována centrální autoritou [11]. Do klíčových vlastností této kryptoměny je možné zahrnout anonymitu, integritu, dostupnost a průhlednost. Finanční operace uskutečněné v rámci interakce komunikujících stran jsou postupně ověřovány a vkládány do distribuovaného řetězce blockchain [10]. Vedle finančního sektoru (kryptoměny) našla technologie blockchain postupně své uplatnění v nejrůznějších sférách lidských aktivit, jako jsou elektronické volby (e-voting), smart contracts, Internet of Things (IoT) a další[2].

Pojmenování technologie blockchain je přímo odvozeno od její vnitřní struktury. Ta se skládá z bloků dat propojených mezi sebou [10]. Technické realizace návaznosti dílčích bloků řetězce blockchain je docíleno použitím hašovací funkce. Její aplikování umožňuje vytvořit unikátní otisk datové části bloku [10, 11]. Do hlavních vlastností hašovacích funkcí patří jednosměrnost, pevná délka (nezávislá na objemu vstupních dat), silná propojenost změn vstupních dat s výstupem funkce a bezkoliznost statisticky limitovaná délkou haše.

[2] O technologii blockchain je možné se podrobněji dočíst v článku „Testování blockchainových řešení“, DSM 4/2019.



Obr. 2: Princip fungování architektury blockchain s MHT [1,2,10]

Propojení jednotlivých bloků dat mezi sebou je uskutečněno vložením hašovacího otisku bloku Bn do hlavičky následujícího Bn+1 bloku (viz obr. 2). Taková struktura umožňuje ukládat řetězec transakcí, které v budoucnu, tj. po provedení uzavření bloku a spočítání jeho hašovacího otisku, již nebude možné změnit [10]. Stejně jako technologie CT používá i blockchain za účelem zefektivnění vkládání a ověření transakcí (viz obr. 2) ve svém základu Merkle Hash Tree (MHT).

Za zmínku stojí skutečnost, že samotné slovo transakce použité ve výše uvedeném významu může, ale také nemusí souviset výhradně s převodem finančních prostředků. Příkladem je platforma Ethereum, která dovoluje vkládat do blockchain tzv. chytré kontrakty (Smart Contracts). Tento potenciál tvoří z blockchain univerzální datovou strukturu, která umožňuje uchovávat v čase se měnící stav sledovaných entit [1,11].

Integrace technologie blockchain do PKI

Při přímém srovnání technologie blockchain a PKI s Certificate Transparency je zřejmé, že se jedná o dva odlišné pohledy na uspořádání a delegování vnitřních procesů v počítačových systémech. V případě výše zmiňované PKI s Certificate Transparency jde o čistě centralizovaný pohled na řízení procesů, ve kterém se fungování celého systému

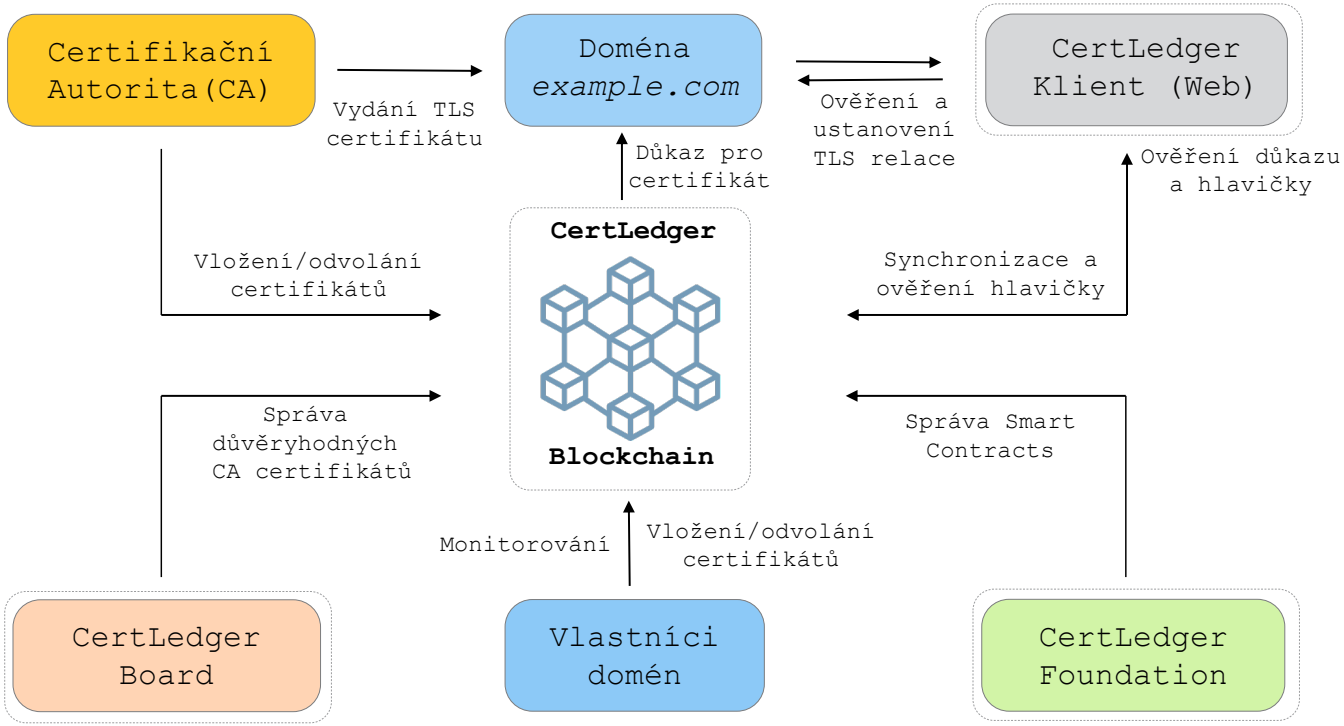
bezprostředně odvíjí od důvěryhodnosti hlavní certifikační autority [3]. Pokud dojde k podvržení garantu důvěry, dojde k zhroucení bezpečnosti celého systému [1,2]. Na druhou stranu je řešení blockchain založené na decentralizovaném přístupu Peer to Peer (P2P) sítě, kde žádný z uzlů není řízen nadřazeným prvkem [10]. Tím se dostáváme k logické otázce, zda by nebylo efektivní kombinovat tyto dvě technologie s cílem zvýšit finální bezpečnosti PKI.

V posledních dvou letech se objevilo poměrně velké množství vědeckých prací, které se dané problematiky dotýkají a na základě volně dostupných blockchain platforem, jako je např. už zmíněná Ethereum, dosahují konkurenceschopných PKI řešení. Současné způsoby integrace je možné rozdělit na dvě základní skupiny. Do té první spadají metody, které koncept existence hlavní certifikační autority nemění, tzn. zachovávají hierarchické uspořádání systému PKI. Tyto metody jsou založené na vývoji podpůrných mechanismů sloužících ke snížení bezpečnostních požadavků kladených na CA (Single Point of Failure) a k docílení transparentnosti během procesu vydání certifikátů, viz [1, 2].

Druhá skupina je tvořena metodami, které se primárně soustředí na decentralizaci klasického PKI systému a jeho koncepční přiblížení k Pretty Good Privacy (PGP). Tyto systémy plně integrují technologii blockchain do hlavních procesů a tvoří systémy typu dPKI (decentralized PKI) [12].

V případě našeho textu klademe důraz na soubor řešení, jejichž motivací není změna hierarchického uspořádání systému PKI, ale jeho posílení se zachováním centralizovaného přístupu. Jedním z ukotvujících bodů pro implementaci technologie blockchain je už několikrát zmiňovaná technika Certificate Transparency [1, 2]. Konkrétně se jedná o realizaci veřejně dostupného úložiště logů se

Architektura PKI Blockchain řešení CertLedger



Obr. 3: Architektura řešení CertLedger [1]

zachováním všech bezpečnostních požadavků a vyřešení nedostatků Certificate Transparency od Googlu.

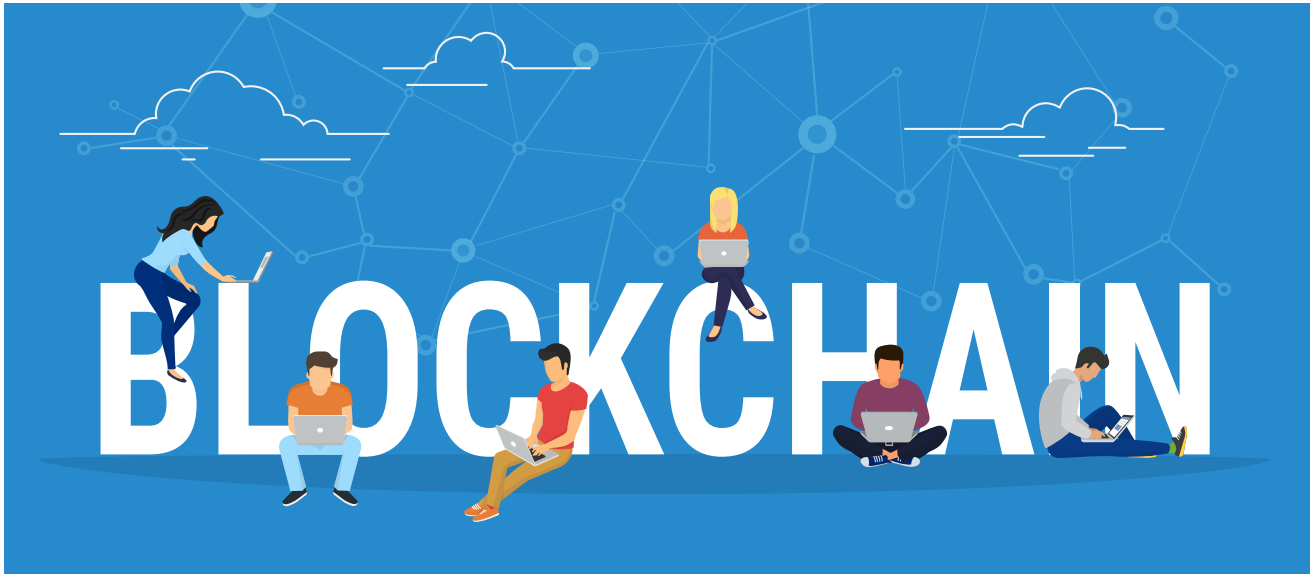
K nejlépe propracovaným řešením vycházejícím z CT patří v současné době CertLedger, viz [1]. Za zmínku také stojí CTB (Hyperledger) a IKP (Ethereum). Decentralizovanými řešeními jsou např. BlockQuick (Ethereum) a Certcoin (Namecoin). Řešení CertLedger (CL) je založeno na síti Ethereum a nabízí zlepšenou architekturu PKI, která vychází z Certificate Transparency a klade důraz na zajištění plné transparentnosti, a to jak během vydávání certifikátů, tak i při jejich revokaci [1].

CertLedger (CL) byl poprvé prezentován v roce 2018 a v současné době je rozšiřován o podporu IoT. Do základních vlastností technologie je možné zařadit odolnost vůči split-world a MITM útokům, transparentnost, efektivní monitorování všech certifikátů, zlepšení bezpečnosti a sjednocení ověřovacího postupu u různorodých TLS klientů [2]. Funkcionalita PKI je v CertLedger realizována pomocí tzv. stavových objektů integrovaných do blockchain [1]. Každý objekt má unikátní adresu a tvoří digitální dokument obsahující data a chytrý kontrakt. Ten slouží k jeho řízení a přístupu k vnitřním informacím.

Principiálně se model CertLedger ke klasickému PKI s Certificate Transparency velmi blíží. V modelu se vyskytují tři druhy entit: externí entity (CA, vlastníci domén), blockchain entity (Miners, Full Nodes) a CertLedger entity (CL Board, CL Foundation, CL Clients (TLS klienti)) [1]. Funkcionalita CA je v CertLedger rozšířena o možnost vytvoření transakce na přidání záznamu o vydání nového certifikátu do CL blockchain nebo změně stavu vydaného certifikátu (jeho revokace). Na druhou stranu CA neprovádí vydání CRL (Certificate Revocation List) a neposkytuje OCSP servisy.

Vlastníci domén nabízejí služby koncovým klientům a kromě standardních akcí provádějí i vložení obdržených certifikátů do CertLedger blockchain (volitelně), monitorují stav svých certifikátů a v případě detekce zkompromitovaného certifikátu jej revokují a vloží patřičný záznam do CL. Těžaři (Miners) validují transakce vložené do blockchain, vytvářejí nové bloky a distribuují je v rámci P2P sítě [10]. Full nodes disponují řetězcem všech transakcí vložených do systému a generují MHR pro ověření TLS klienty. Klienti CertLedger jsou light TLS klienty, kteří jsou schopni validovat a ukládat hlavičky bloků CL spolu s MHR. Po provedení všech validačních kroků jsou klienti schopni navázat bezpečné TLS spojení s příslušnou doménou. Dalšími specifickými entitami pro řešení CertLedger jsou CL Board a CL Foundation [1].

Hlavní vlastností členů množiny CL Board je distribuce úrovně důvěry mezi několika entitami PKI a spravování množiny certifikátů všech certifikačních autorit. Technicky je řízení příslušných certifikátů realizováno přes stavový objekt Trusted CA State Object v kombinaci s prahovým mechanismem určujícím míru svévolnosti CA [1]. Z bezpečnostních důvodů by množina entit CL Board měla být zastoupena světově



uznávanými organizacemi, např. IEEE, ISO, IETF atd. Hlavní úlohou CL Foundation je podpora CL platformy spočívající ve vývoji a rozvoji daného řešení. Entita CL Foundation navíc vlastní inicializační CL token, detailněji viz [1].

Závěr

Klasická realizace PKI bez implementace dodatečných bezpečnostních mechanismů není odolná vůči sofistikovaným útokům souvisejícím se zneužitím certifikační autority (2009 – Null prefix attack, 2010 – Stuxnet, 2015 – Symantec, 2015 – Let's Encrypt, 2017 – Symantec, 2018 – Certinomis, 2018 – GoDaddy). O útocích je možné se detailněji dočíst ve zdrojích [1, 4]. Tento předpoklad by měl posloužit jako motivace pro významné dodavatele IT služeb a IT organizace včetně PKISO (PKI Standards Organisations), k implementaci nových bezpečnostních mechanismů a neustálému zlepšování systémů PKI.

Řešení, která dnes existují na základě technologie blockchain, jsou již dostatečně ověřená a mohou posloužit jako vhodná alternativa nebo jako vylepšení klasického PKI modelu. K jejich přednostem patří hlavně vysoká bezpečnost, efektivita a škálovatelnost. K prohloubení znalostí a vytvoření širšího přehledu o současných trendech a způsobech integrace uvedených dvou technologií doporučujeme další odborné texty, především v anglickém jazyce [1, 2].

Vysvětlení klíčových pojmů (textbox)

Útok typu split-world

Jedná se o cílený počítačový útok, který je možné úspěšně aplikovat na infrastrukturu veřejných klíčů (PKI) už zesílenou technikou Certificate Transparency [1]. Útočník se při něm snaží napadenému subjektu podvrhnout podobu stromu logových záznamů (CL) prostřednictvím zkresleného Merkle Hash Proof. Nedetekovatelnosti lze docílit současným napadením certifikační autority a úložiště logů. Úspěšná realizace útoků je umožněna především tím, že ověřovací strana není v přijatelném čase schopna zkontrolovat všechny větve vývoje distribuovaného logového úložiště a vždy přistupovat k aktuální verzi MHT [1].

Zero Trust

Bezpečnost infrastruktury organizací optikou Zero Trust byla poprvé koncipována Johnem Kindervagem v roce 2010. Jeho pojetí zahrnovalo Zero Trust Network a Zero Trust Architecture [13]. Hlavní myšlenkou bylo zajištění úplné transparentnosti a neposkytování automatické důvěry žádnému subjektu uvnitř ani vně hranic firemní sítě. V praxi to znamená, že jakákoli aktivita interagující s infrastrukturou subjektu musí být monitorována a vyžaduje autentizaci.

Merkle Hash Tree (MHT)

Jedná se o stromovou datovou strukturu, tzv. binary hash tree, která se často používá v kryptografii a informatice. Leží v základu P2P systémů a takových platforem, jako jsou Bitcoin, Ethereum, Apache Cassandra DB, GitHub, GitLab a další. Umožňuje rychlou kontrolu integrity dat použitím hašovací funkce a hierarchického uspořádání prvků [2].

Ethereum

Ethereum představuje decentralizovanou open-source platformu v jejímž základu leží blockchain. Oproti bitcoinu je výpočetní síť Ethereum postavena na chytrých kontraktech Smart Contracts). Ethereum nabízí turingovsky virtuální stroj (Ethereum Virtual Machine), který lze použít k provozu různorodých decentralizovaných aplikací.

Yehor Safonov
yehor.safonov@aec.cz

Bc. Yehor Safonov

Je studentem dvou prezenčních magisterských programů: Informační bezpečnost (Vysoké učení technické v Brně) a Aplikovaná informatika (Masarykova univerzita v Brně). Zároveň je zaměstnancem společnosti AEC, a. s., kde pracuje na pozici Security Specialist se zaměřením na návrh a implementaci bezpečnostních monitorovacích řešení typu SIEM pro rozsáhlé počítačové infrastruktury. Pilíř jeho zájmů tvoří počítačová bezpečnost, kryptografie, teoretická informatika a moderní techniky strojového učení.

POUŽITÉ ZDROJE

[1] KUBILAY, Murat Yasin, Mehmet Sabir KIRAZ a Haci Ali MANTAR. *CertLedger: A New PKI Model with Certificate Transparency Based on Blockchain* [online]. 2018, 43 str. [cit. 2020-03-12]. Dostupné z: https://eprint.iacr.org/2018/1071.pdf
[2] JHANWAR, Mahabir Prasad, Anupam CHATTOPADHYAY a MADALA. *Certifcate Transparency Using Blockchain* [online]. 2018, 19 str. [cit. 2020-03-12]. Dostupné z: https://eprint.iacr.org/2018/1232.pdf
[3] ALBARQI, Aysha, Ethar ALZAID, Fatimah Al GHAMDI, Somaya ASIRI a Jayaprakash KAR. *Public Key Infrastructure: A Survey* [online]. [cit. 2020-03-13]. Dostupné z: https://pdfs.semanticscholar.org/7794/69761ec8782a5c3f2ed2db9d0ea43a1ff523.pdf
[4] Timeline of Certificate Authority Failures. *SSLMATE* [online]. [cit. 2020-03-13]. Dostupné z: https://sslmate.com/certspotter/failures
[5] MAZIERES, David, Dennis SHASHA. *Building secure file systems out of byzantine storage*. In Proceedings of the twenty-first annual symposium on Principles of distributed computing, pages 108–117. ACM, 2002
[6] CHUAT, Laurent, Pawel SZALACHOWSKI, Adrian PERRIG, Ben LAURIE a Eran MESSERI. *Efficient gossip protocols for verifying the consistency of certificate logs* [online]. [cit. 2020-03-13]. Dostupné z: https://www.scion-architecture.net/pdf/2015-gossip.pdf
[7] DOWLING, Benjamin, Felix GUNTHER, Udyani HERATH a Douglas STEBILA. *Secure Logging Schemes and Certificate Transparency* [online]. 2016, 27 str. [cit. 2020-03-12]. Dostupné z: https://eprint.iacr.org/2016/452.pdf
[8] *How Certificate Transparency Works* [online]. [cit. 2020-03-13]. Dostupné z: http://www.certificate-transparency.org/how-ct-works
[9] CROSBY, Scott, Dan WALLACH. *Efficient data structures for tamper-evident logging*. In USENIX Security Symposium, str. 317–334, 2009.
[10] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash systém* [online]. 2008 [cit. 2020-03-13]. Dostupné z: https://bitcoin.org/bitcoin.pdf
[11] ZHENG, Zibin, Shaoan XIE a Hong-Ning DAI. *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends* [online]. 2017 [cit. 2020-03-13]. Dostupné z: https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends
[12] LETZ, Dominic. *BlockQuick: Super-Light Client Protocol for Blockchain Validation on Constrained Devices* [online]. 2019 [cit. 2020-03-13]. Dostupné z: https://eprint.iacr.org/2019/579.pdf
[13] KINDERVAG, John. What is Zero Trust? *Paloalto Networks* [online]. [cit. 2020-04-30]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture