

Přenos dat, počítačové sítě a protokoly

Reputační systémy

Doc. Ing. Petr Matoušek, PhD., M.A.



Fakulta informačních technologií VUT v Brně

matousp@fit.vutbr.cz

Na stupnici 0 – 10 ohodnoťte důvěru danému člověku.



Jaké hodnocení 0 – 10 byste dali následujícím filmům?



Obsah přednášky

- 1 Důvěra
 - Důvěra a reputace
 - Reputační systémy
 - Síťový reputační systém
- 2 Příklady reputačních systémů
 - PageRank
 - Cisco Talos Reputtion
 - NERD
 - Další systémy
- 3 Rizika reputačních systémů
 - Soukromí
 - Čínský kreditový systém
- 4 Literatura

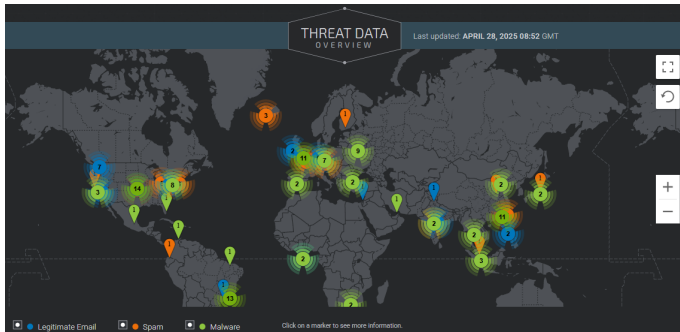
Důvěra na Internetu

Problém důvěry (nejen na Internetu)

Proč hledáme globální mechanismus důvěry na Internetu (provoz, uživatelé, zdroje)?

- **Emaily:** spamy, podvržené emaily, phishing
- **Webové služby:** podvržené stránky, stránky s malwarem, nevhodný obsah
- **Sdílení softwaru:** zavirované soubory, malware
- **Síťové spojení:** ochrana sítí proti zneužití (botnety, útoky DDoS)

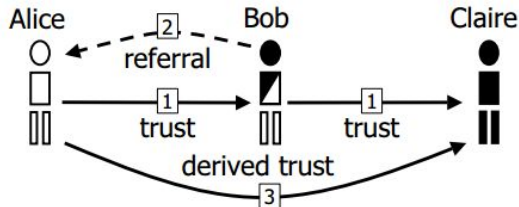
Příklad: [Cisco Talos Reputation Center](#)



Důvěra

Co je důvěra?

Důvěra (trust) = asymetrická, tranzitivní relace, která vyjadřuje důvěryhodnost či spolehlivost jedné entity (*truster*, důvěřující) vůči druhé (*trustee*, nositel důvěry)[1].



Příklad důvěry:

Banka (důvěřující) se rozhoduje, zda poskytne zákazníkovi (nositeli důvěry) úvěr, který zákazník splatí. Podstatou důvěry je tvrzení (*assertion*) o nositeli důvěry.

- Říkáme, že důvěřující (*truster*) důvěřuje nositeli důvěry (*trustee*), pokud očekává, že dostane peníze zpět.
- Nositel důvěry je důvěryhodný (*trustworthy*), pokud půjčku splatí.

→ Podle čeho pozná banka, zda je zákazník hodný důvěry?

Důvěra

Jak poznáme, že je daná entita hodná důvěry?

- Důvěřující často nezjistí důvěryhodnost nositele důvěry přímo, ale hledá znaky důvěryhodnosti, tzv. *signál*.

→ **Co může být signálem?**

Signál = aktivita nebo vlastnost, kterou může důvěryhodná entita jednoduše splnit, ale jejíž získání je pro nedůvěryhodnou entitu příliš drahé.

Prospěchář (*opportunist*): entita, která není důvěryhodná, ale která napodobuje znaky důvěryhodnosti s cílem zlepšit svou důvěryhodnost.

⇒ **Pozor na prospěcháře!**



Reputace

Co je reputace (reputation)?

⇒ Znak důvěryhodnosti vyjádřený svědectvím dalších entit.

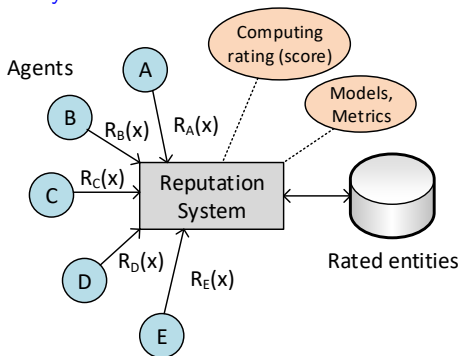
- Efektivní rozlišující signál, který podporuje spolupráci postavenou na důvěře.
- Reputace není dokonale rozlišující signál.
- Reputace je efektivní, pouze pokud jsou svědectví nezávislá a důvěryhodná.
- Reputace je založena na zkušenostech, historii či vztazích.

Co je potřeba k budování důvěry? [2]

- 1 Informace vhodné pro měření důvěry a reputace v daném systému důvěry.
- 2 Metrika pro výpočet reputace (reputation score) či míry risku (risk rating):
 - Různé algoritmy pro výpočet hodnoty reputace.
 - Hodnocení závisí na aktuálních i historických zkušenostech.
- 3 Způsob získání a udržování těchto informací:
 - centralizovaný či distribuovaný reputační systém.
- 4 Reputační systém musí být odolný vůči manipulaci.

Reputační systémy

Architektura reputačního systému

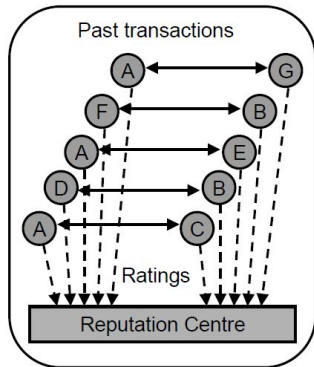


- Hodnotitelé (reputation agents) zasílají hodnocení entity x (rating, evaluation).
- Reputační systém spočítá reputační skóre (rating).
 - Bere v úvahu důvěryhodnost hodnotitelů, historii hodnocení apod.
- Pro výpočet využívá různé metriky i modely hodnocení.
- Kvalita hodnocení závisí na vstupních datech i způsobu výpočtu.

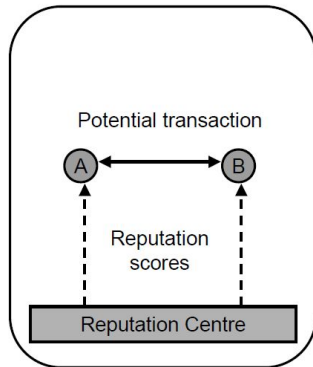
Reputační systémy

Centralizovaný reputační systém

- Hodnotitelé předávají hodnocení do jednoho centrálního systému.
- Systém vyhodnocuje reputaci na základě vstupních hodnocení a dalších informací.
- **Příklad:** hodnocení reputace na základě hodnocení minulých transakcí.



a) Past

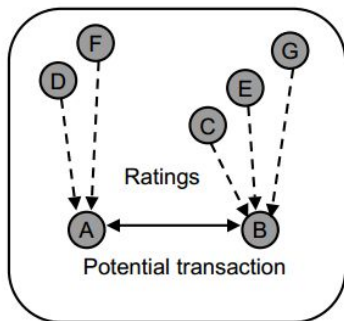
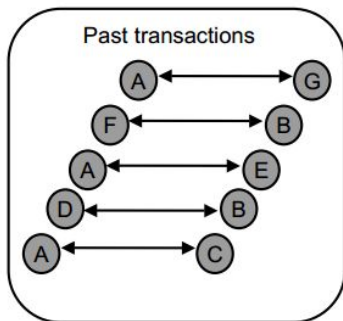


b) Present

Reputační systémy

Distribuovaný reputační systém

- Pro výměnu hodnocení se využívá spolehlivý partner (relaying party).
- Tento partner počítá reputační skóre na základě získaných hodnocení.
- Využívá se například u sítí P2P pro hodnocení spolehlivosti uzlu.



Reputační systémy

Jak vypočítat hodnotu reputace?

- 1 Součet jednotlivých hodnocení uživatelů
 - eBay's Feedback Forum: $R = \sum_i \text{positive_score}_i - \sum_j \text{negative_score}_j$
 → Co je lepší: 100 pozitivních + 10 negativních reakcí nebo 90 pozitivních?
- 2 Průměr jednotlivých hodnocení
 - Amazon: počítá spokojenost na stupnici 1-5, bere průměr hodnocení.
- 3 Bayesovské systémy
 - Vstupem je binární hodnocení (pozitivní či negativní).
 - Reputační skóre se počítá pomocí rozdělení pravděpodobnosti Beta.
 - Hodnocení (α, β) , kde α je počet pozitivních a β negativních hodnocení.
- 4 Modely důvěry (belief models)
 - Model počítá metriky důvěry na základě důvěry, nedůvěry a nejistoty.
 - Tyto názory se mapují na funkci hustoty rozdělení pravděpodobnosti Beta.
- 5 Modely toků
 - Počítají důvěru a reputaci na základě tranzitivity hodnocení účastníků.
 - Například algoritmus PageRank (Google), Appleseed či Advogato.

Reputační systémy

Příklad reputačního systému Beta [3]

- Slouží k výpočtu důvěry na základě předchozí zkušenosti (zpětné vazby).
- Využívá rozdělení pravděpodobnosti Beta, které reprezentuje binární události.

Příklad: Pokud má proces A výstupy $\{a, \bar{a}\}$ a výstup a nastal $8x$ a výstup \bar{a} nastal $2x$, jaká je pravděpodobnost, že v budoucnu dostaneme na výstupu a ?

→ Náhodnou veličinou u rozdělení Beta je pravděpodobnost.

Rozdělení pravděpodobnosti Beta

- Spojité rozdělení na intervalu $[0, 1]$ pro vyjádření pravděpodobnosti budoucích událostí.
- Hustota rozdělení pravděpodobnosti závisující na parametrech α, β :

$$f(p|\alpha, \beta) = \frac{p^{\alpha-1}(1-p)^{\beta-1}}{B(\alpha, \beta)}, \text{ kde funkce } B(\alpha, \beta) = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}, E(p) = \frac{\alpha}{\alpha+\beta}$$

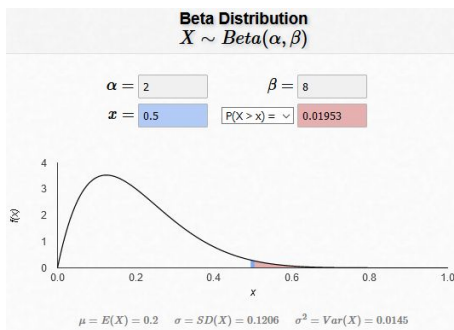
- Rozdělení Beta je podobné binomickému rozdělení $f(x) = \binom{n}{x} p^x \cdot (1-p)^{n-x}$.
 - Binomické rozdělení popisuje výskyt náhodného jevu x v n pokusech při pravděpodobnosti jevu p .
 - Rozdělení Beta reprezentuje pravděpodobnost úspěšného pokusu p , kde $(\alpha - 1)$ označuje počet úspěšných a $(\beta - 1)$ počet neúspěšných pokusů.

Reputační systémy

Rozdělení pravděpodobnosti Beta

Příklad: Mějme počet úspěšných pokusů $\alpha = 2$, počet neúspěšných pokusů $\beta = 8$. Jaká je pravděpodobnost, že úspěšný pokus x nastane s 50% pravděpodobností?

- Hledáme hodnotu rozdělení Beta: $f(p(X > 0.5)|2, 8)$
- Výsledek $f(p|\alpha, \beta)$ je 0,01953 = 1.95%



- Pokud $\alpha = \beta$, pak rozdělení Beta odpovídá normálnímu rozdělení.

Reputační systémy

Reputační systém Beta [3]

- Vypočítává pro dané parametry α, β reputační skóre na základě výskytu předchozích zkušeností (zpětné vazby).
- Předpokládejme, že $\alpha = r + 1$ vyjadřuje pozitivní a $\beta = s + 1$ negativní zkušenosti.
- **Reputační funkce** φ entity T (target) na základě zkušeností r_T a s_T :

$$\varphi(p|r_T, s_T) = \frac{1}{B(r_T + 1, s_T + 1)} \cdot p^{r_T} \cdot (1-p)^{s_T} = \frac{\Gamma(r_T + s_T + 2)}{\Gamma(r_T + 1) + \Gamma(s_T + 1)} \cdot p^{r_T} \cdot (1-p)^{s_T}$$

- **Reputační skóre** Rep = normalizovaná střední hodnotu rozdělení v intervalu $[0, 1]$:

$$Rep(r_T, s_T) = (E(\varphi(p|r_T, s_T)) - 0.5) \cdot 2 = \frac{r_T - s_T}{r_T + s_T + 2}$$

Další rozšíření výpočtu reputačního skóre Rep :

- Kombinovaná zpětná vazba od více agentů: $r_T = r_T^x + r_T^y$, $s_T = s_T^x + s_T^y$.
- Přidání reputace agentů (opinion): $\omega = (b, d, u)$ (belief, disbelief, uncertain)
- Faktor zapomínání λ : $r_T = \sum_{i=1}^n r_{T,i} \lambda^{n-i}$, $s_T = \sum_{i=1}^n s_{T,i} \lambda^{n-i}$

Sítový reputační systém

- Reputace je služba založená na ohodnocení → není to černá listina.
- Reputace vyjadřuje, jak „rizikové“ je komunikovat s daným uzlem.
- Reputace je časově podmíněná.

⇒ Skóre sítového reputačního systému vyžaduje dobře vysvětlenou interpretaci hodnoty.
Např. uzel A posílá spamy s pravděpodobností 54%.

Sítový reputační systém

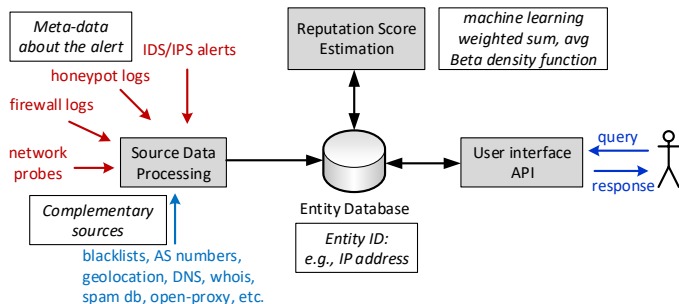
- Sítový reputační systém poskytuje platformu pro monitorování aktivit v síti.
- Sbírá data ze sítových senzorů, firewallů, IPS zařízení, anti-virové analýzy apod.
- Provádí korelaci dat a počítá hodnotu reputace či míru risku.
- Při výpočtu bere v úvahu historická data.

Jaká data lze použít pro výpočet reputace?

- záznamy z logů firewallu či IDS, např. IP adresu a port útočníka
- velikost IP datagramu, hodnoty z hlavičky TCP (MSS, options)
- počet žádostí o příchozí či odchozí spojení
- otisk zprávy, seznam spammerů, URI, reverzní záznamy z DNS a další

Architektura reputačního systému

Obecná architektura síťového reputačního systému



Vstupní data pro hodnocení síťových uzlů:

- data o detekovaných útocích či anomáliích: IDS/IPS, honeypoty, sondy, firewally,
- blacklisty škodlivých IP adres, URL, domén či AS, bad neighbourhood (/24),
- whitelisty, seznamy open-proxy stanic, databáze spamů,
- informace o provozu: IP adresy, doménová jména, URL, velikosti paketů,
- internetové databáze: DNS, Whois, geolokace, apod.

Komunikace v reputačním systému

Komunikace reputačního systému dle RFC 7070 [4]

- Model klient – server.
- *Reputační klient*: chce ohodnotit daný obsah (např. e-mail) na základě zájmového identifikátoru (například jména domény odesilatele).
- *Reputační služba*: sbírá a ukládá reputační data, počítá skóre, odpovídá klientům.

Zasílání dotazů od klienta dle RFC 7072 [5]

- Dotaz obsahuje ID klienta, název aplikace (kontext, např. e-mail), předmět dotazu.
- Reputační služba definuje šablonu dotazu (template) ve formátu HTTP URI.
- Příklad formátu: `http://service/application/subject/assertion`

Příklad dotazu:

- # - klient se dotazuje na doménu "example.com" v kontextu "email-id"
- # - dotaz je poslán na reputační službu "rep.example.net"
- # - klient žádá ohodnocení tvrzení, zda je doména hodnocena jako "spam"

`http://rep.example.net/email-id/example.com/spam`

Komunikace v reputačním systému

Reputační služba

- Zpracuje dotaz od klienta: vyhledá a spočítá reputační skóre pro daný identifikátor.
- Vytváří reputační odpověď (reputon) týkající se hodnocení.
- [RFC 7071](#) definuje strukturu odpovědí ve formátu application/reputon+json:

Content-Type: application/reputon+json # příklad odpovědi reputační služby

```
{
  "application": "email-id",          # aplikační kontext - např. hodnocení odesilatele e-mailu
  "reputons": [                      # seznam hodnocení
    { "rater": "rep.example.net",     # entita, která poskytuje hodnocení dotazu (reputační služba)
      "assertion": "spam",           # tvrzení, pro které hledáme ohodnocení - spam/abusive/fraud/malware
      "identity": "dkim",            # způsob hodnocení: služba DKIM (DomainKeys Identified Mail)
      "rated": "example.com",        # předmět hodnocení - doména, kterou hodnotím vůči tvrzení "spam"
      "confidence": 0.95,             # úroveň důvěry reputační služby v poskytnuté pro hodnocení: 95%
      "rating": 0.012,                # reputační skóre z intervalu 0-1: s pravděpodobností 1.2% je to spam
      "sample-size": 16938213,       # počet hodnot použitých pro výpočet skóre
      "updated": 1317795852
    },
    { "rater": "rep.example.net",     # hodnocení stejné domény pomocí jiného kritéria
      "assertion": "spam",
      "identity": "spf",              # využití služby SPF (Sender Policy Framework)
      "rated": "example.com",
      "confidence": 0.98,             # důvěra v hodnocení: 98%
      "rating": 0.023,                # reputační skóre pro tvrzení "spam" je 2,3%
      "sample-size": 16938213,
      "updated": 1317795852
    }
  ]
}
```

Vlastnosti reputačního systému

Vlastnosti síťového reputačního systému

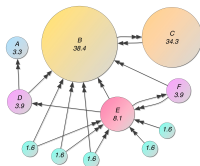
- Větší granularita hodnocení oproti blacklistům
→ binární dělení vs. interval reputace.
- Možnost vyjádřit důvěru v hodnocení (confidence).
- Oproti blacklistům poskytuje dodatečné informace.
- Korelace více typů zdrojových dat včetně historických dat.
- Umožňuje odhadnout predikci budoucího chování.
- Detekuje regiony (neighbourhoods) dobrého či špatného chování.

Ochrana dat reputačního systému

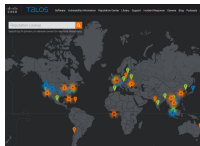
- Reputační systém může obsahovat citlivé údaje o uživatelích, stanicích, doménách.
- Ochrana dat při komunikaci - neveřejné informace (pomocí HTTPS či S/MIME).
- Přístup k reputačnímu systému - pouze autorizovaní klienti (dotazy, vkládání dat).
- Vytváření reputace bez předsudků (unbiased reputation agents).

Příklady reputačních systémů

- **PageRank:** hodnocení webových stránek



- **Cisco Talos Reputation Center:** hodnocení e-mailů, webových služeb, souborů



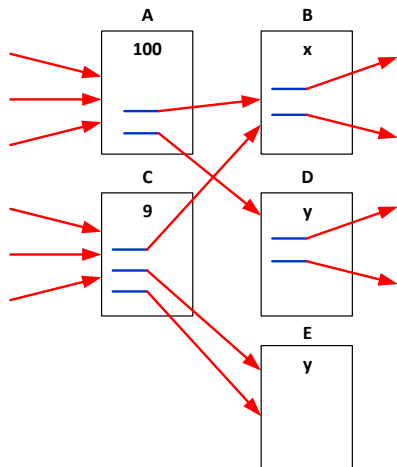
- **Network Entity Reputation Database (NERD):** - predikce škodlivého chování



PageRank: hodnocení webových stránek

Úloha: Jak hodnotit důležitost webových stránek?

- Propojení webových stránek odkazy URL lze zobrazit ve formě orientovaného grafu.
- Důležitost stránky A odpovídá důležitosti stránek, které na ni odkazují.

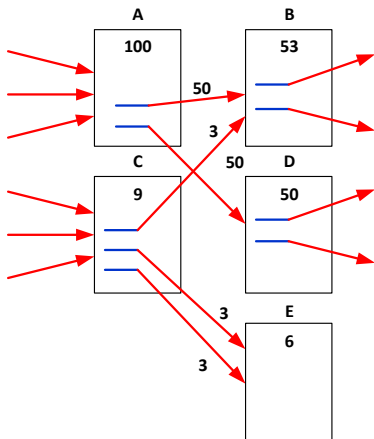


- Předpokládejme hodnocení $A=100$, $C=9$.
- Jaké bude hodnocení stránek B, D a E?
- Uvažujme pouze počet odkazů na stránku.
 - Hodnocení B je stejné jako hodnocení E.
 - Hodnocení D je menší než hodnocení E.
- ⇒ Prostý počet odkazů nestačí.
- ⇒ Potřeba uvažovat i váhu stránek.
 - Váha odkazu bude záviset na hodnocení stránky, ze které vede.
 - Váha bude normalizována počtem všech odkazů ze stránky.

PageRank: hodnocení webových stránek

PageRank – hodnocení důležitosti webové stránky (ranking) [6]

- Necht' F_u je množina stránek odkazovaných ze stránky u , $N_u = |F_u|$ je jejich počet.
- Necht' B_u je množina stránek, které se odkazují na u .
- Důležitost stránky u závisí na počtu odkazů z B_u a jejich vahách.



- Hodnocení důležitosti stránky (ranking):

$$R(u) = c \sum_{v \in B_u} \frac{R(v)}{N_v}$$

kde c je faktor normalizace.

- Např. $R(B) = \frac{R(A)}{2} + \frac{R(C)}{3} = 50 + 3 = 53$.
- Hodnocení bere v úvahu nejen počet odkazů, ale i jejich kvalitu.
- Hodnocení se počítá rekurzivně → problém s inicializací a cyklickými odkazy.

Implementováno v roce 1998 na Stanfordu do jednoduchého vyhledávacího stroje zvaného Google.

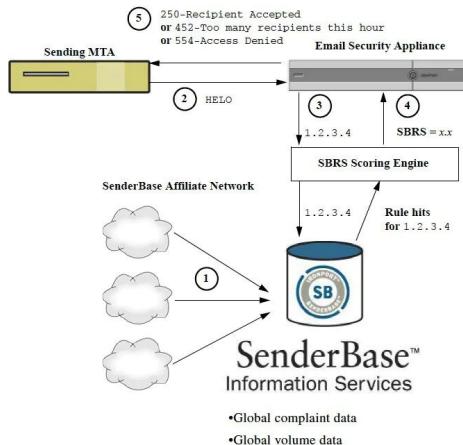
Cisco Talos Reputation Center

Reputace e-mailů Cisco Talos Reputation (dříve SenderBase)

- Systém vyvinut firmou IronPort, dnes součástí [Cisco Talos Intelligence](#).
- Reputační databáze pro hodnocení e-mailů, webových služeb, malwaru.

Jak systém pracuje?

- Sbírá data z více jak 100.000 sítí ve světě (IPS, firewally, e-mail/web appliances).
- Vstupní parametry: objem přenesené pošty, open-proxy IP, URL využívané pro spamy a viry, špatně doručené e-maily, konfigurace DNS, blacklisty, whitelisty, počet hopů, webcrawler, země původu.
- 200 váhovaných atributů pro hodnocení.
- **Reputační skóre odesilatele (dle IP adres): -10 až 10.**
- Filter zahazuje e-maily s hodnotou < -3.
- Na základě hodnocení se vytváří tzv. reputační filtry pro zařízení Cisco.



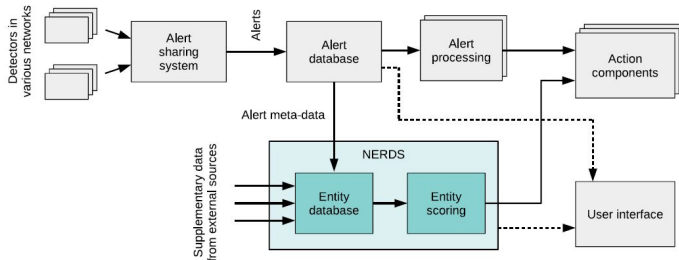
Systém NERD

Network Entity Reputation Database (NERD) System [7]

- Vyvinut na CESNETu, viz [veřejná část NERD](#).
- Obsahuje hodnocení škodlivých zařízení na síti na základě IP adresy.
- Počítá predikci škodlivého chování Future Misbehaviour Probability (FMP).
- Získává data z honeypotů, zařízení IDS, síťových analyzátorů, logů, apod.

Vstupní data:

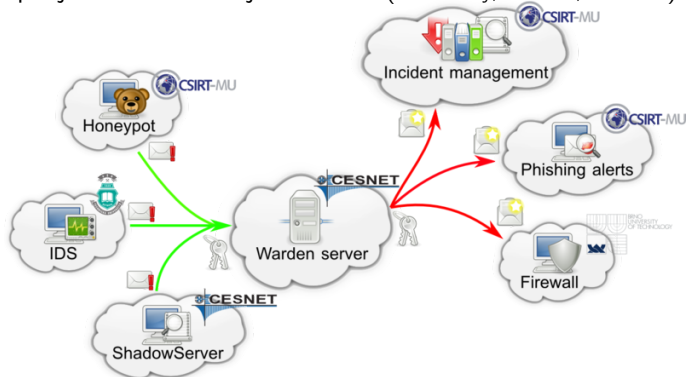
- **meta data**: alerty z detektorů v síti CESNET či systému [MISP](#).
- **doplňková data**: registrace doménového jména, číslo AS, whois, geolokace, blacklisty, databáze [DShield](#).



Systém NERD – vstupní data

Warden: systém pro sdílení bezpečnostních incidentů

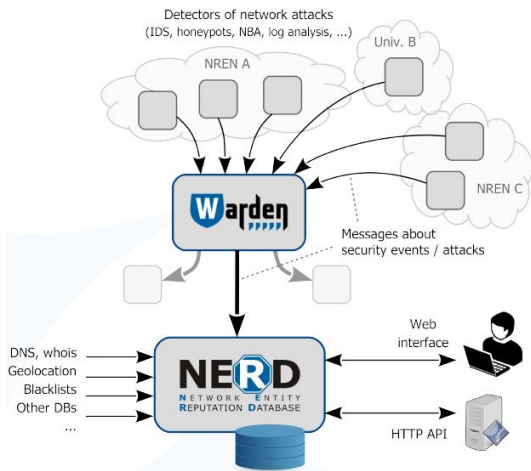
- Architektura klient-server, přispívající a odebírající klienti.
- Formát data: [IDEA](#).
- Velikost databáze: 64.8 GB.
- Frekvence: 1.5 mil. událostí/den.
- 17 přispívajících a 23 odebírajících klientů (univerzity, CSIRT, CZ.NIC).



Systém NERD – zpracování dat

IP address record:

- Timestamp: creation, last update
- All reported events
- Hostname
- Country, city
- ASN, abuse contact
- Blacklists
- Amplifier (open DNS, NTP,...)
- TOR exit node
- [Shodan info](#) (open ports)
- Static/dynamic address
- Device type
- Reputation score



Systém NERD – výpočet reputace

Definice událostí

- Událost $a = (t, e, c, v, d)$, kde t je čas události, e je identifikátor entity (např. IP adresa), c je kategorie události, v je množství událostí, d je detekční systém.
- Hledáme predikci chování v budoucnu $T_p(t_0, t_0 + w_p)$, kde w_p je šířka okna.

Definice chování entity

- Pro danou entitu e určíme **vektor atributů** $\vec{x}_{e,t_0} = (x_1, x_2, \dots, x_n)$ v čase t_0 , kde x_i :
 - počet alertů, celkový počet událostí, počet detektorů, čas poslední události
 - interval mezi událostmi: průměr [EWMA](#) (Exponentially Weighted Moving Average)
 - Systém NERD používá celkově 58 různých atributů [7].

Výpočet reputačního skóre FMP (Future Misbehaviour Probability) [7] = klasifikace

- Třída $y_{e,t_0} = 1$ iff $\exists a \in A : a = (t, e, \dots, \dots), t \in T_p$, tj. pokud nastane událost a v čase T_p , pak patří do třídy 1, jinak patří do třídy 0 (binární klasifikace).

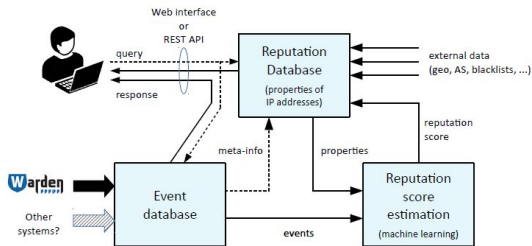
$$\hat{y}_{e,t_0} \approx p(y_{e,t_0} = 1 | \vec{x}_{e,t_0}).$$

⇒ Odhad tvoří **reputační skóre**, tj. $FMP(e, t_0) = \hat{y}_{e,t_0}$.

Model podmíněné pravděpodobnosti p se vytvoří z trénovací množiny pomocí strojové učení s učitelem (neuronové sítě NN2, NN3 a rozhodovací stromy GBDT) [7, 8].

Systém NERD – použití systému

Využití reputace k ohodnocení entit (IP adres)



Příklady dotazů [9]:

- Jaké je hodnocení IP adresy $x.y.z.a$?
 - Je to známý spammer.
 - Často zkouší útoky hrubou silou na SSH.
 - Před týdnem prováděl skenování, od té doby nic.
 - Jedná se o botnet server podle blacklistu X.
 - Neznámá adresa, pravděpodobně neškodná.
- Vypiš škodlivé IP adresy z mé podsítě 147.229.0.0/16.
- Vypiš otevřené DNS resolvers, které se podílely na útoku typu DNS amplification.

Další příklady reputačních systémů

McAfee URL Ticketing System

- Provádí reputaci souborů (ochrana proti malware), webu a e-mailů.
- Zkoumá domény e-mailů, hodnocení webových serverů v dané doméně.
- Pro výpočet reputace uzlů zkoumá IP adresy, čísla portů a komunikující protokoly.
- Ukládá si historii domén a další informace.

Barracuda Reputation System

- Reputace IP adres a doménových jmen pro hodnocení odesilatele e-mailů.
- Použito pro spamový a virový filtr BRBL (Barracuda Reputation Block List).
- Používá historii IP adres, data z honeypotů a analýzu e-mailových spojení.
- Detekuje spammery a open-relay servery.

SenderScore

- Vytváří profil odesilatele e-mailů.
- Počítá skóre 0 (nejhorší) až 100 (nejlepší) na základě informací "return path".
- Vstupem jsou hodnocení z mailových serverů ISP a spamových filtrů.
- Skóre se počítá v 30denním plovoucím okně.

Rizika reputačních systémů

Soukromí (privacy) – pohled do historie

- George Orwell: **1984**, vydáno 1949.
- Ray Bradbury: **451° Fahrenheita**, vydáno 1953.
- Kádrový posudek pracujícího (komplexní hodnocení), 1948-1989, např. [zde](#).
- Jaký je cíl systémů pro "reputaci" ?

Dnešní situace ohledně soukromí (privacy)

- Současné technologie umožňují sběr velkého množství dat o aktivitách člověka.
→ "Track Everything About Everyone at All Times" [10].
- Data získávána ve spolupráci státních orgánů i soukromých společností.
- Proces sběru data není vždy viditelný a transparentní.
→ Kdo sbírá jaká data, za jakým účelem, jak je využívá, jak dlouho je uchovává?

Možné "využití" dat

- hodnocení "spolehlivosti" člověka = kompatibilita s pravidly společnosti
- reklamní a komerční účely, cílená reklama, obchodní nabídky
- sledování politických názorů, ovlivňování voličů
- personalizovaný přístup: sledování informací o konkrétním člověku, profilování

Čínský kreditový systém

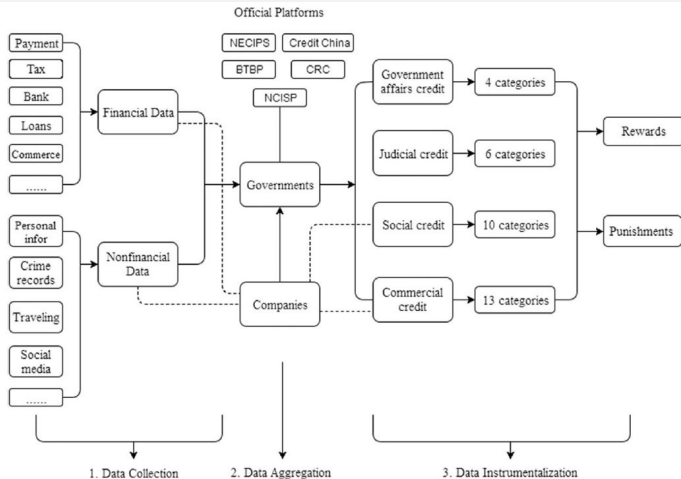
Čínský kreditový systém (Social Credit System, SCS)

- 2007 - Koncept sociálního kreditového systému pro hodnocení finanční spolehlivosti.
 - Databáze kreditového hodnocení podniků a osob, Čínská lidová banka.
- 2014 - Plán tvorby sociálního kreditového systému (2014-2020), Státní rada ČLR.
 - Hodnocení nejen finančního kreditu, ale i společenského chování.
 - Systém odměn (red list) a postihů (black list).
- Pilotní projekty (2005-2019) [11]
 - Soukromé: Sesame Credit (Alibaba), Tencent Credit, Kaola Credit.
 - Státní: města Šen-čen, Chang-čou, prefektura Suej-ning, Peking, Šanghaj.
- 2015 - Národní platforma pro sdílení kreditových dat.

Co je cílem navrženého systému?

- Prosazení morálních hodnot: upřímnost (chengxin) a důvěryhodnost (yongxin).
- Systém sleduje dodržování zákonů a nařízení firem i jednotlivců.
- Vychází z učení Konfucia – jak vytvořit ideální státní zřízení [12].
- Kredit = důvěra, spolehlivost, čestnost státních úředníků i občanů.

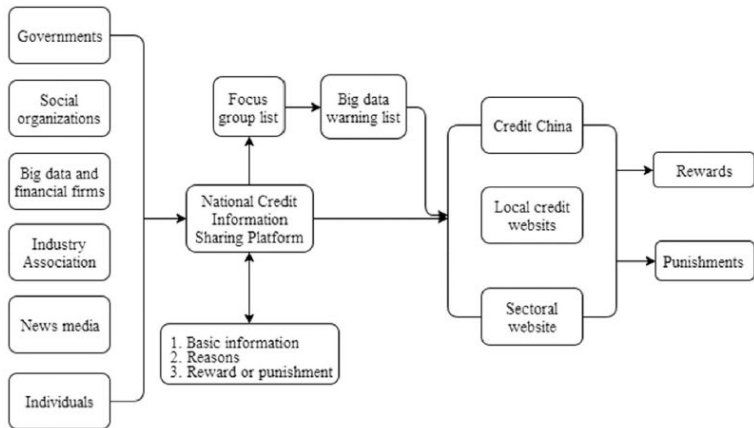
Čínský kreditový systém - architektura [10]



- **Vstupní data:** finanční i nefinanční data, státní i soukromé databáze.
- **Zpracování dat:** národní platforma pro sdílení dat, výpočet kreditu.
- **Použití dat:** odměny (red list) a postihy (black list).

Čínský kreditový systém

Tok dat v kreditovém systému [10]



- **Odměny:** vládní podpora, půjčky, prioritní vyřizování záležitostí, slevy.
- **Postihy:** omezený přístup k vládní podpoře, cestování, nákup nemovitostí, vzdělání.

Čínský kreditový systém

Zhodnocení systému

- Centralizace datových zdrojů na státní úrovni.
- Využití pokročilých technologií pro získání a zpracování dat.
- Navázání na služby státu i komerčních subjektů.
- Jak přijímají tento systém lidé v Číně? → Viz studie [13].

Reputační systémy v našem životě

- Jaká jsou rizika a přednosti reputačních systémů?
- Kdo má právo zpracovávat a využívat shromažďovaná data?
- Jaký je postoj společnosti?

Reputace v životě člověka:

- Jaká je moje reputace?
- Kdo ji buduje a na čem záleží?
- Jak ovlivňuje můj život?

Použitá literatura

- [1] Tom Slee. Some Obvious Things About Internet Reputation Systems. 2013.
- [2] Audun Jøsang, Roslan Ismail, and Colin Boyd. A Survey of Trust and Reputation Systems for Online Service Provision. *Decis. Support Syst.*, 43(2):618–644, March 2007.
- [3] Audun Jøsang and Roslan Ismail. The Beta Reputation System. In: *Proceedings of the 15th Bled Conference on Electronic Commerce*, page 14, 01 2002.
- [4] N. Borenstein and M. Kucherawy. *An Architecture for Reputation Reporting*. IETF RFC 7070, November 2013.
- [5] N. Borenstein and M. Kucherawy. *A Reputation Query Protocol*. IETF RFC 7072, November 2013.
- [6] Lawrence Page, Sergey Brin, Rajeev Motwani, and Terry Winograd. The PageRank Citation Ranking: Bringing Order to the Web. Technical Report 1999-66, Stanford InfoLab, November 1999. Previous number = SIDL-WP-1999-0120.
- [7] Vaclav Bartos, Martin Zadnik, Sheikh Mahbub Habib, and Emmanouil Vasilomanolakis. Network entity characterization and attack prediction. *Future Generation Computer Systems*, 97:674–686, 2019.
- [8] Mohammad Samar Ansari, Vaclav Bartos, and Brian Lee. Shallow and Deep Learning Approaches for Network Intrusion Alert Prediction. *Procedia Computer Science*, 171:644–653, 2020.
- [9] Václav Bartoš. Creating a Network Reputation Database. In *Proceedings of the Terena Network Conference*, page 1, 2016.
- [10] Fan Liang, Vishnupriya Das, Nadiya Kostyuk, and Muzammil M. Hussain. Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet*, 10(4):415–453, 2018.
- [11] Rogier Creemers. China's Social Credit System: An Evolving Practice of Control. *SSRN Electronic Journal*, May 2018.
- [12] Martin Chorzempa, Paul Triolo, and S. Sacks. China's Social Credit System: A Mark of Progress or a Threat to Privacy? *Policy briefs*, 2018.
- [13] Genia Kostka. China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, 21(7):1565–1593, 2019.