Anonymní komunikace na internetu

PV080

Motivace pro anonymitu

- Ochrana osobních dat
- Anonymita uživatele, lokace, transakce
- 4 funkčnosti systémů pro ochranu inf. soukromí
  - anonymita
  - pseudonymita
  - nesledovatelnost
  - nepozorovatelnost

Motivace pro anonymitu

- Nutnost zajistit anonymitu v mnoha případech
  - informace o zdravotním stavu (anonymita vs. pseudonymita)
  - elektronické volby
  - svoboda slova
  - udání informací o trestné činnosti apod.

Anonymita vs. pseudonymita

- Anonymita – chování zcela anonymní, neexistuje možnost zjištění skutečné identity subjektu
  - např. informace o zdravotním stavu bez vazby na identitu skutečného pacienta
- Pseudonymita – chování je anonymní, existuje možnost zpětného zjištění skutečné identity subjektu
  - stanovení diagnózy – jednoznačné spojení s pacientem
  - lékař zná pouze nějaké ID pacienta
  - v systému existují záznamy (ID, jméno), ke kterým ale ošetřující lékař nemusí mít přístup

Anonymita – rub a líc

- Zneužití útočníkem
  - útočník je velmi těžko zpětně zjistitelný

- Systémy pro poskytnutí anonymity chrání před krádeží identity

Definice anonymity – opak.

- Společná kritéria – standard pro hodnocení bezpečnosti systémů
  - uživatel může využít zdroj nebo službu bez odhalení své identity
- Mixovací systémy
  - stav bytí neidentifikovatelným v rámci dané množiny subjektů, tzv. anonymitní množině
    - s ohledem na možného odesílatele zprávy
    - s ohledem na možného příjemce zprávy
- Význam modelu útočníka
  - pasivní/aktivní, lokální/globální
  - anonymitu vyjadřujeme s ohledem na model útočníka

Charakteristiky anonymity

- Kvantitativní – velikost anonymitní množiny
  - různá pro odesílatele/příjemce
  - různé přístupy pro určování anonymitní množiny
  - nelze brát v úvahu pouze velikost množiny
  - potřeba zohlednit i „chování“ subjektů
- Kvalitativní – odolnost vůči různým útokům

Zpoždění komunikace

- Použití systému pro poskytování komunikace zvyšuje latenci
  - V případě mixů velmi výrazně
  - V případe Onion routingu (a spol.) méně výrazně
- Cena za anonymní komunikaci
  - Podle ní pak využití email, www, ...
- V některých případech lze částečně ovlivnit
  - Stop-and-go mixy
  - Onion routing – volba cest s menším počtem uzlů
  - Ale s vlivem na míru poskytnuté anonymity

Typy útoků na anon. systémy

- Analýza provozu – nejběžnější pasivní útok
  - snaha útočníka zjistit kdo s kým komunikuje
  - pasivní sledování provozu na síti
  - profilování účastníků komunikace
  - statistické metody pro omezení velikosti anonymitní množiny
- Falešný provoz v síti – obrana proti analýze provozu
  - kompenzace malého provozu v síti
  - maximalizace datového provozu a počtu uživatelů zvyšuje „kvalitu“ poskytované anonymity

Motivace pro mixy

- Internetový provoz vysledovatelný, data svázána s jejich odesilatelem
- Mixy – routery měnící tok a výskyt dat (zpráv) na komunikačním kanálu
  - vstupy nelze jednoduše spojit s výstupy
  - skrytí obsahu zpráv: **kryptograficky**
  - úplné skrytí komunikujících partnerů
  - změna toku zpráv: prodlevy, přeuspořádání, falešné zprávy
  - vyvážení hladiny přípustného zpoždění/ceny vs. míry poskytnuté anonymity

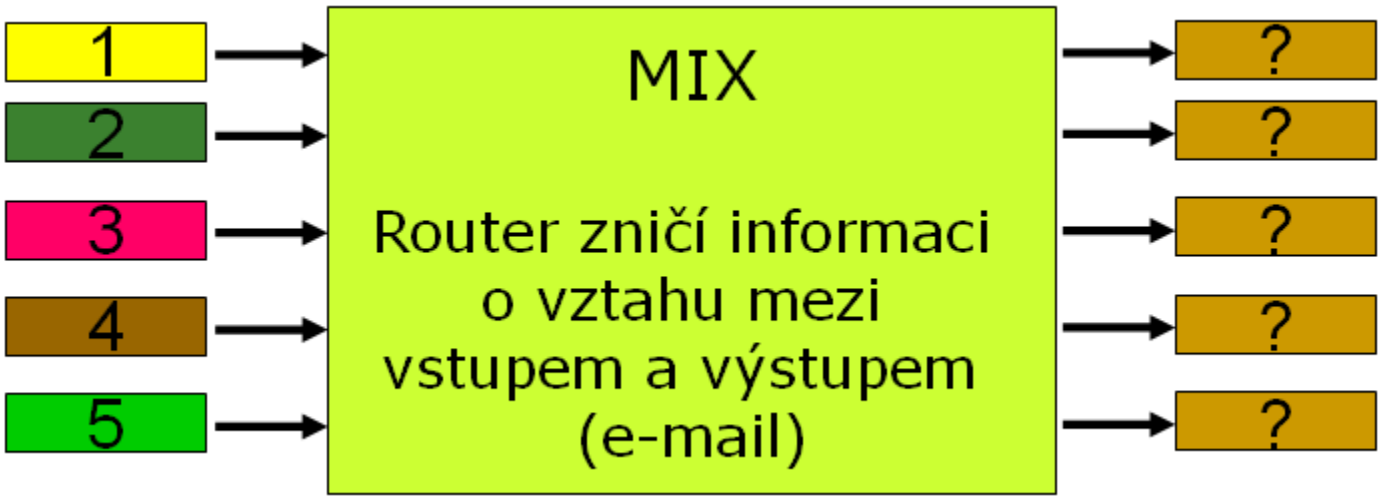
Anonymní email

- Broadcastové sítě – filozofie doručení zpráv všem, lze šifrovat pro vybrané(ho)
  - Anonymita příjemce
- („anonymní“) remailer třídy 0
  - V podstatě pseudonymita a nespojitelnost příjemce s odesilatelem, udržování tabulky pseudonymů
- („anonymní“) remailer třídy 1 – řízení činnosti příkazy

Typy mixů

- David Chaum – Chaum/prahový (threshold) mix (1981)
  - shromáždí N zpráv
  - přeuspořádání zpráv
  - odeslání zpráv (fire/flush)
  - informace o spojení odesilatel-příjemce je zničena
  - zpráva je v mixu typicky také „přešifrována“

Typy mixů


1
2
3
4
5
MIX
Router zničí informaci o vztahu mezi vstupem a výstupem (e-mail)
?
?
?
?
?

Typy mixů

- Pool mixy: rozšíření původního návrhu přidáním vnitřní paměti
  - zprávy jsou zpracovány v dávkách
  - různé podmínky pro odeslání zpráv
    - časová/prahová
    - deterministická/nedeterministická
  - algoritmus pro výběr zpráv z paměti
    - statická paměť; dynamická paměť
    - ovlivňuje výkon a míru poskytované anonymity

Typy mixů

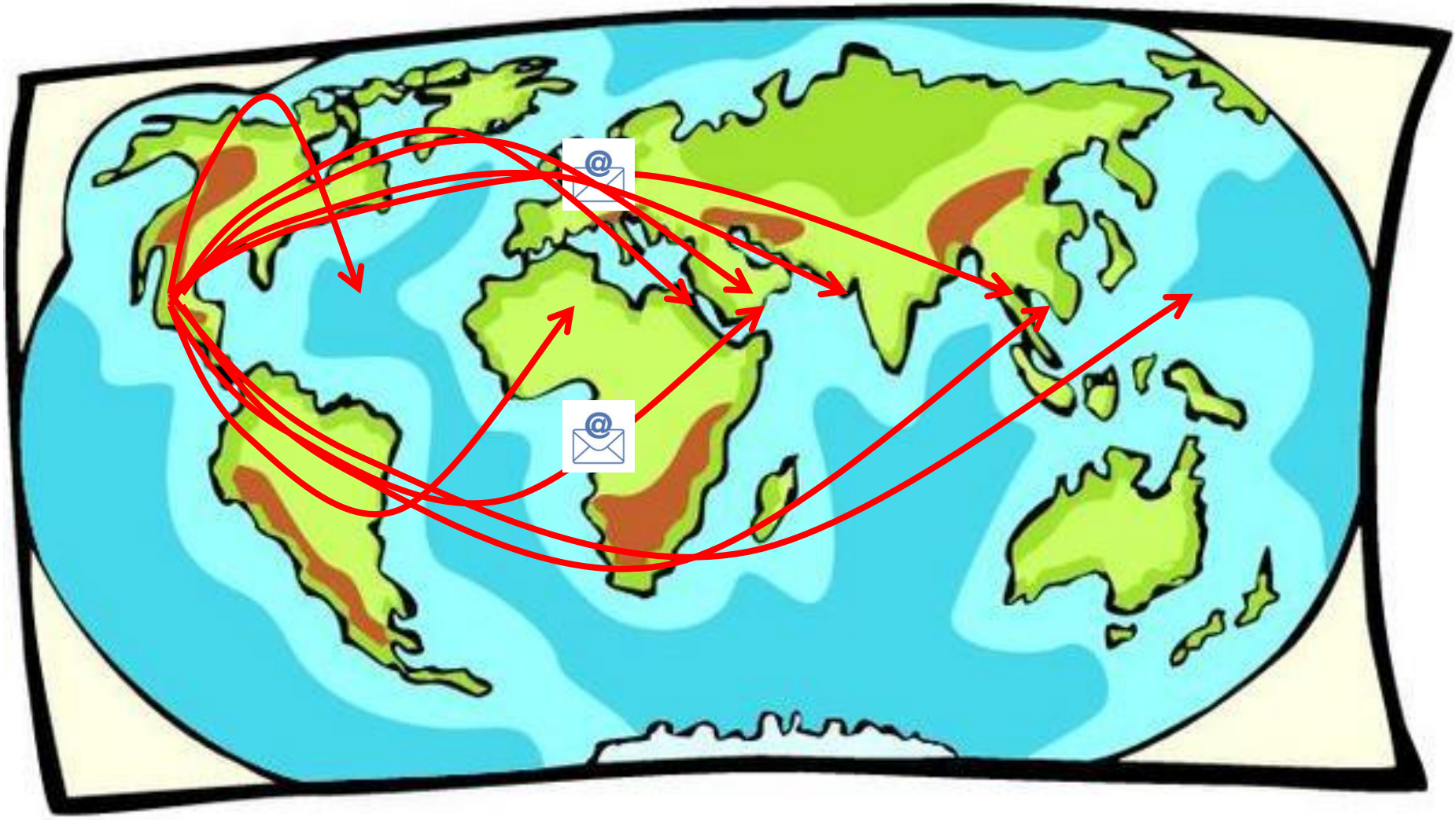
- Continuous/stop-and-go mixy
  - mixování založené na prodlevách
  - zprávy jsou po určitou dobu pozastaveny v mixu
  - problém při malém provozu na síti
  - uživatel má možnost ovlivnit prodlevy
  - musí existovat služba poskytující informace o mixech pro uživatele

Typy mixovacích sítí

- Dobré nespoléhat pouze na jeden mix
- Uzly se často spojují do mixovacích sítí
  - zapojení jako síť mixů – nerestriktivní směrování (uživatel sám volí cestu)
  - zapojení jako „kaskáda mixů“ – omezení směrování (uživatel musí použít tuto cestu)
  - hybridní zapojení
    - několik kaskádových cest v síti – uživatel volí
    - volba sousedních mixů – mix určí množinu svých možných následníků, uživatel si náhodně jeden zvolí

Dummy traffic (umělý provoz v síti)

- Potřeba pro:
  - zvýšení odolnosti proti vybraným útokům
  - kompenzace malého provozu na síti
  - zvýšení anonymity
  - poskytnutí nevystopovatelnost
- Falešné zprávy (fake messages)
  - generují uživatelé/mixy, mixy je zahazují
  - útočník nerozezná falešnou zprávu od skutečné



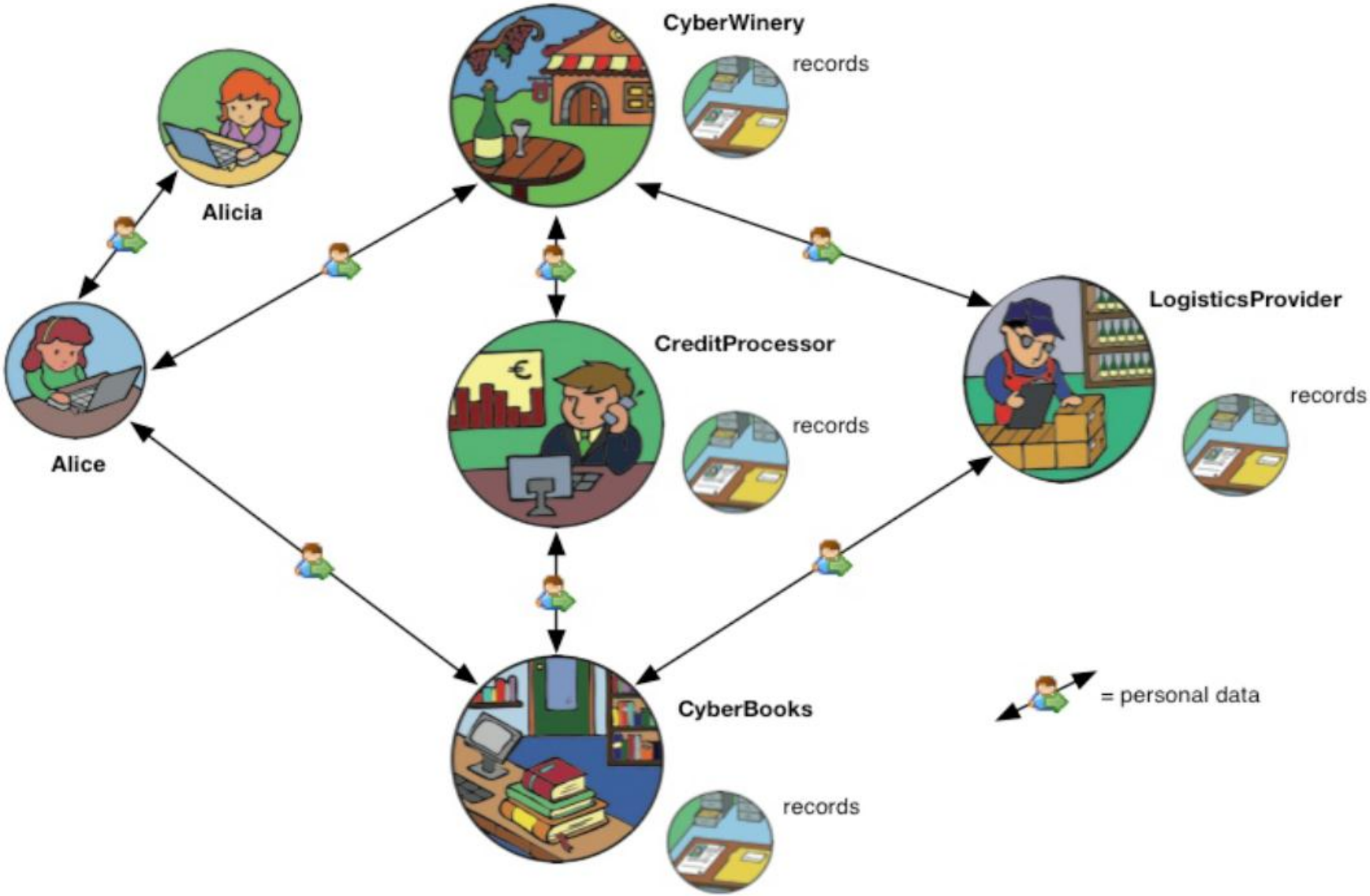
Měření anonymity

- Anonymitní množina
  - množina uživatelů, kteří mohli poslat danou zprávu – anonymitní množina odesílatele
  - stejně pro příjemce
- Velikost množiny jako takové není dobrý ukazatel
  - různé chování uživatelů (odesílatelů/příjemců)
- Entropie – použití pro určení velikosti množiny
  - zohledňuje pravděpodobnost provedení akce
- Vhodné zohlednit kontextové informace se vztahem ke zkoumanému systému
  - časy odeslání zpráv, četnost zpráv, velikost zpráv, ...

PRIME project

- Projekt se zabývá ochranou soukromých informací při online komunikaci
- Zejména pak toku těchto informací ve vybraných aplikacích
- Cílem projektu bylo navrhnout mechanizmy pro ochranu inf. soukromí
- Návrh prostředí, kdy uživatelé mají kontrolu nad šířením informací o sobě

PRIME – prostředí



Projekt PRIME

- Obrázek znázorňuje tok osobních dat typický pro online obchodování
- Při registraci zákazníka obchod sleduje předchozí objednávky – využití při doporučeních
- Registrací může obchodník získat např. i informace o platební kartě
  - Nalákání zákazníka na snazší vyřízení budoucích objednávek
- V případě, že dodávku zboží vyřizuje ext. firma (příp. platby), tak tyto subjekty také získají data zákazníka
- Možnost propojení dat v případě objednávky např. knih, kdy dodávky a platby zpracovává stejná dodavatelská firma

Projekt PRIME

- Data zákazníka jsou uložena v několika databázích
- Možnost dalšího zpracování dat pro obchodní účely
- LogisticProvider např. ví, co, kdy a kde si Alice koupila
- Náročná kontrola zpracování osobních dat z pohledu Alice
- Nebezpeční zneužití dat, krádež identity...
- Cílem projektu PRIME je navrhnout řešení některých problémů z představeného scénáře

Cíle PRIME

- Poskytnout uživatelům „prostředí“ pro lepší kontrolu svých osobních dat
- Prime toolbox – tvorba, použití, sledování použití digitálních identit a přidružených atributů
- Princip minimalizace dat – poskytnout pouze nezbytně nutná data

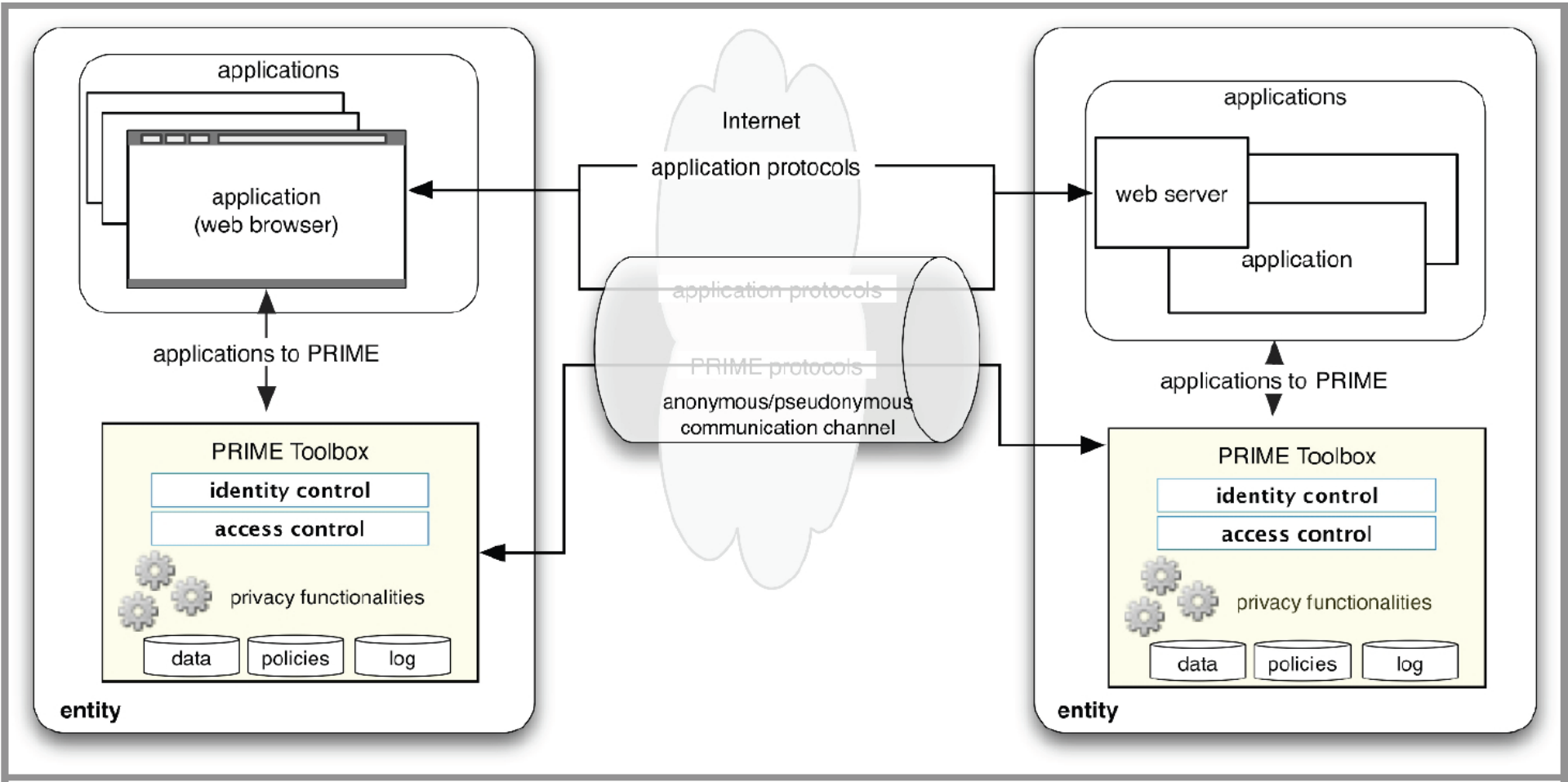


Figure 2: PRIME high level architecture

Pohled zákazníka

- Proč bych měl obchodníkovi věřit?
  - Jen proto, že má pěkný web?
  - Důvěryhodná třetí strana?
- Jak je zabezpečená komunikace s obchodníkem?
- Jasně stanovené podmínky pro zpracování dat zvyšují důvěryhodnost
  - Proč obchodník potřebuje osobní data
  - Co se s daty stane po dokončení nákupu?

Objednávka zboží

- Nutnost poskytnout data potřebná pro doručení zásilky
  - Zdlouhavé pročítání informací o zpracování dat; „specifický“ styl popisu;
  - Z pohledu zákazníka většinou nicneříkající text
  - Zákazník typicky zaškrtne „souhlasím s podmínkami“ a další text nečte

Objednávka zboží

- Pohled PRIME – privacy policy negotiation
  - zákazník v PRIME consoli zvolí své preference (např., že nechce dostávat reklamní emaily)
  - PRIME console prověří politiku obchodníka a zákazníkovi předloží např. unifikované rozhranní pro zadávání potřebných informací
  - PRIME console také udržuje seznam obchodníků a poskytnutých dat pro lepší orientaci zákazníka

Pravdivost údajů

- Podpora tzv. private credentials
- Hlavní „certifikát“ subjektu obsahující řadu informací
  - Poskytnutí určité informace (např. zda je kupující plnoletý), takovým způsobem, že tato informace je ověřitelná jako např. občanský průkaz
- Prodejce nemusí znát adresu, pokud zboží expeduje někdo jiný
  - Alice pošle zašifrovaný token, ale dešifrovací klíč bude mít jen expediční firma

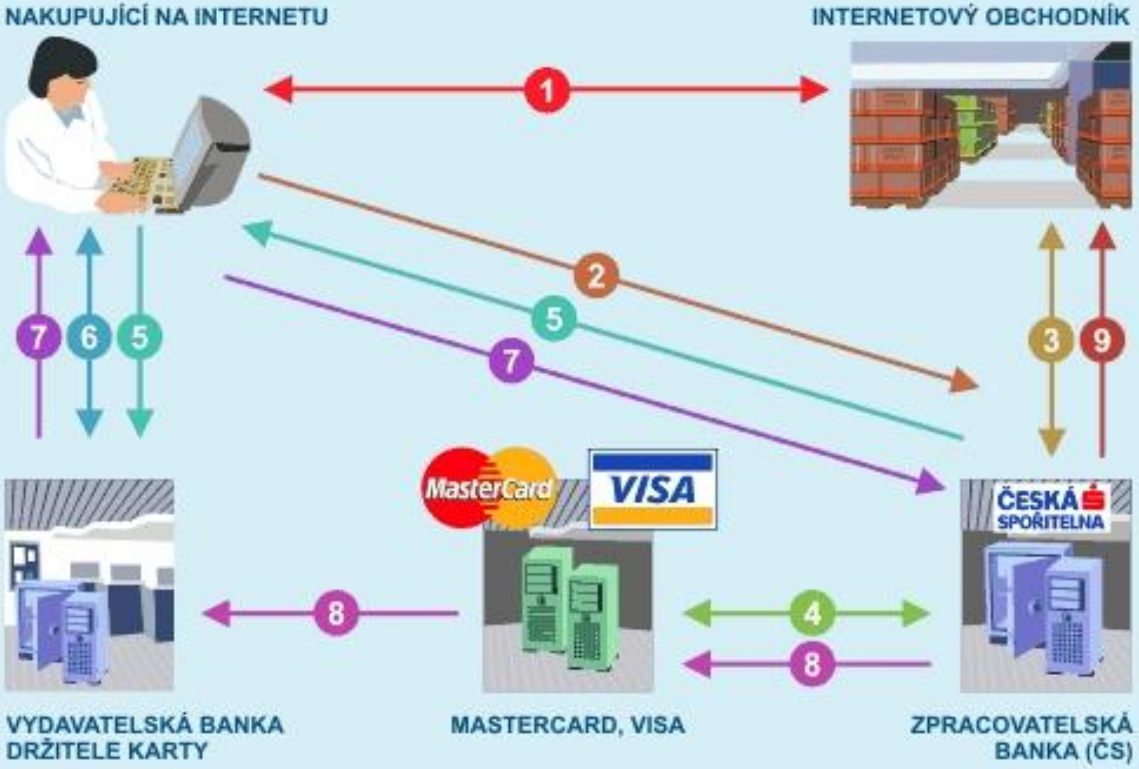
PRIME DataTrack

- Udržuje seznam použitých pseudonymů a informace o tom, jaká data byla (a komu) pod tímto pseudonymem poskytnuta
- Umožňuje zákazníkovi určitou kontrolu
- Též pomáhá při ověření, jaké informace obchodník o zákazníkovi uchovává
  - Na toto ověření má zákazník nárok
- Vynucení politiky na straně obchodníka
  - Prostřednictvím PRIME Middleware
  - Smazat adresu po odeslání zásilky
  - Smazat veškeré údaje z databáze po *n* měsících, pokud je to takto uvedeno v podmínkách obchodníka

Jiné řešení pro ochranu os. údajů

- 3D-secure systém pro realizaci bezh. plateb
- Vyvinula VISA, později se připojil MasterCard
- Autentizační mechanizmus pro bezhotovostní platby kartou
- Ochrana proti zneužití platební karty
- Obchodník je pouze informován o úspěšně provedené transakci
- Validitu platební karty ověřuje přímo banka, nikoliv obchodník

3D SECURE



1. Zákazník navštíví internetový obchod a vybere si zboží nebo službu.
2. Po potvrzení vybraného zboží je nakupující přesměrován na ČS, kde zadá platební údaje.
3. Odsouhlasení objednávky mezi ČS a obchodníkem.
4. ČS vyšle dotaz na kartovou asociaci. Asociace (VISA, MasterCard) potvrdí zařazení/nezařazení držitele karty do systému 3D-Secure a pošle odpověď zpátky do ČS.
5. ČS pošle žádost na autentizaci (ověření) karty do vydavatelské banky přes prohlížeč držitele karty.
6. Vydavatelská banka požádá držitele karty o heslo. Držitel karty vyplní heslo a banka toto heslo potvrdí.
7. Vydavatelská banka pošle odpověď zpátky do ČS přes prohlížeč držitele karty.
8. V případě, že autentizace proběhla úspěšně, je internetová platba dále zpracována jako běžná platební transakce.
9. ČS zašle obchodníkovi informaci o výsledku transakce.

Pozn.: V případě, že držitel karty není zařazen do systému 3D-Secure, transakce proběhne bez autentizace držitele karty. Zodpovědnost za případné zneužití karty nese vydavatelská banka.

Převzato z materiálů ČS, a.s.