Identita a online hrozby

Václav Matyáš, Marek Kumpošt, PV080

"On the Internet, nobody knows you're a dog."

Russian hackers steal more than 1 billion passwords 08/2014

"…Initially, the gang acquired databases of stolen credentials from fellow hackers on the black market. These databases were used to attack e-mail providers, social media, and other websites to distribute spam to victims and install malicious redirections on legitimate systems. Earlier this year, the hackers altered their approach. Through the underground black market, the CyberVors got access to data from botnet networks. These botnets used victims' systems to identify SQL vulnerabilities on the sites they visited. The botnet conducted possibly the largest security audit ever. Over 400,000 sites were identified to be potentially vulnerable to SQL injection flaws alone…"

Or was it just a lesson from social engineering?

Was **YOUR** identity compromised?

Identita

Libovolná podmnožina atributů určitého jedince, která tohoto jedince jednoznačně určuje v jakékoliv množině jedinců

Existuje více identit jedince, v závislosti na prostředí

Částečná identita se vztahuje k určitému kontextu, roli, nebo omezené množině jedinců

Identifikace mezi osobami v „běžném životě“

Podle čeho identifikujeme známou osobu?

Jméno/příjmení Vzhled Hlas v telefonu Fotografie

Podle čeho identifikujeme neznámou osobu?

Oficiální státní dokumenty Pas Občanský průkaz

Řidičský průkaz Rodné číslo

Dají se tyto atributy identity snadno zjistit/podvrhnout?

Mnoho podob „identity“

Digitalizování atributů pro identifikaci

emailová adresa přezdívky na sociálních sítích mobilní telefon

elektronické dokumenty fotografie otisky prstů

hesla PINy přístupové karty

Fyzická osoba jako soubor digitálních atributů

Kontrola/správa těchto digitálních atributů? subjektem nebo institucemi

Kategorie atributů pro určení identity

Doménové – v rámci práce, školy, zdravotnictví, státních úřadů

Funkční – lokalita, sociální skupina, biologické, psychologicky osobnostní

Dočasné

- *Trvalé-dané* – pohlaví, barva očí, rodiče, datum narození,...
- *Trvalé-získané* – kvalifikace, chování,...
- *Trvale-situační* – adresa, rodinný stav,...
- *Přechodné* – lokace, účes, styl oblékání,...

Kategorie atributů vs. různé znakové sady

Atributy identity zapsané v různých znakových sadách, např. jméno

Marek Kumpošt Марек Кумпошт Marek Kumposht

Μαρεκ Κυμποστ

Jedná se o stejnou osobu, chybu v přepisu – (ne)jednoznačnost?

Identifikace mezi osobami v „online“ prostředí

Podle čeho identifikujeme známou osobu?

Mailová adresa Přezdívka Profil na sociální síti

Podle čeho identifikujeme neznámou osobu?

???

Dají se tyto atributy identity snadno zjistit/podvrhnout?

Identifikace uživatelů vůči službám v „online“ prostředí

Podle čeho identifikujeme známého uživatele?

Login/Heslo/Klíč Token Biometrické údaje

Podle čeho identifikujeme neznámého uživatele?

???

Dají se tyto atributy identity snadno zjistit/podvrhnout?

Osobní identita

Biologická Fyziologická Sociální

Kriminologie předpokládá, že během života člověka se identita nemění

Externí a interní identifikace

Potřeba lepší identifikace – příjmení, identifikační čísla…

Šangaj má 8 mil. Lidí se 408 příjmeními, celá Čína 3 100 příjmení a čínských Top 5 (Zhang, Wang, Li, Zhao, Chen) používá 350 milionů lidí

V ČR např. cca 40k Nováků, 25k Svobodů, 25k Novotných (www.kdejsme.cz)

Identita a online|offline kriminologie

Kriminologie předpokládá, že během života člověka se identita nemění

otisky prstů DNA další biometriky?

Změnit lze řadu věcí jak v osobní identitě, ... (např. v rámci ochrany svědků)

změna jména změna bydliště změna pohlaví

... tak zejména v online identitě

viz obláček na předchozím slajdu

Kriminologie a online (spolehlivá!) identifikace?

Identita a kriminologie – případy/souvislosti

Kolize identit – neúmyslná špatná vazba

Změna identity – záměrně špatná vazba

Delegace identity – se souhlasem

Převzetí identity – bez souhlasu/vědomí

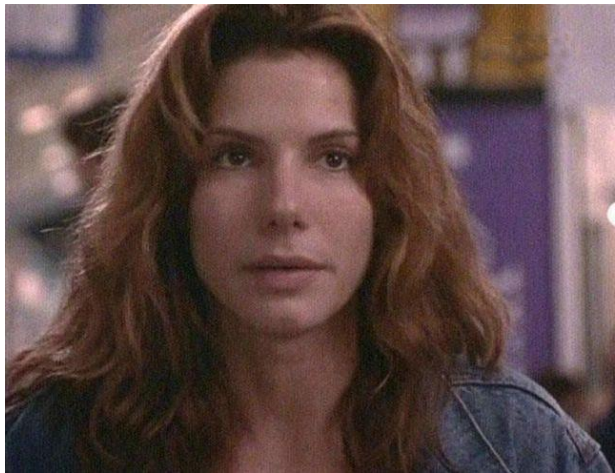
Výměna identity

Vytvoření identity

Zničení identity – vazba je zničena

Obnovení identity – vazba je obnovena

Krádež identity – její převzetí



Wikipedia – Identity – Computer Sci.

Identity – object-oriented programming – describes the property of objects that distinguishes them from other objects

Identity column – database field that uniquely identifies every row in the table and is made up of values generated by the database

Federated identity – assembled identity of a person's user information, stored across multiple distinct identity management systems

Digital identity – representation of a set of claims made by one digital subject about itself or another digital subject

Identity management – administrative area that deals with identifying individuals in a system and controlling access to resources by placing restrictions on them

Online identity – social identity that an internet user establishes in online communities and websites

Celosvětový technologický růst

Milion prodaných počítačů denně (stejné množství tabletů)

Dva miliony prodaných chytrých telefonů denně (téměř 7 mld. aktivních)

Osobní auta připojená na internet, obsahují cca 50 počítačových systémů

„Inteligentní“ domy – pozn. Google např. koupil firmu na výrobu termostatů

Ohromný nárůst komunikace na online sítích za poslední roky

elektronické pasy, eID, RFID, senzorové uzly

http://www.internetlivestats.com/

Opakování důležitých definic

Anonymita	Využití zdrojů a služeb bez odhalení identity
Pseudonymita	Bytí pseudonymním je stav používání pseudonymu jako identifikátoru (ID)
Nespojitelnost	Využití více zdrojů a služeb bez možnosti spojit tato využití do souvislosti s konkrétním uživatelem
Nesledovatelnost	Zamezit možnosti sledovat, že zdroj nebo služba je někým využívána

Poznámky k pseudonymitě

Anonymita a prokazatelná zodpovědnost (accountability) jsou dva extrémy

V praxi obvykle vhodná pseudonymita

- Ovlivňuje spojitelnost mezi předměty zájmu a uživateli

Opakované použití pseudonymu může uživateli umožnit ustavení reputace (důvěryhodnosti)

Uživatelé používají větší počet pseudonymů

- Odhalují spojitost mezi nimi jen v případě potřeby (zisku výhod, času, peněz...)

Ochrana vlastní online identity

Co považujeme za zásadní prvky pro ochranu online identity?

Přístupové údaje – hesla, PINy, klíče

Obsah, který sdílíme online

Ochrana prostředků pro online komunikaci

Ochrana zařízení pro ukládání citlivých informací


"Identity will be the most valuable commodity for citizens in the future, and it will exist primarily online."
Eric Schmidt - Google Chairman
NEWS
LIKE
COMMENTS
FOLLR PROFILE
PHOTOS
VIDEOS
STATUS
TWEET
TWEET
TWEET
follr
follr

Způsoby „získávání“ osobních informací

Odposlouchávání nešifrované síťové komunikace

MITM útoky

Keyloggery – lokální, vzdálené

„Sociálně-inženýrské metody“

- Spam, phishing, přátelé přátel
- …

Nedbalost uživatelů!

Odposlech nešifrované síťové komunikace

Při použití nešifrovaných variant protokolů pro přístup k webovým stránkám, souborům nebo emailům jsou přenášená data čitelná pro kohokoliv, kdo je schopen odposlouchávat provoz.

Odposlech síťového provozu je výrazně jednodušší v bezdrátových sítích. Toto je možné i v situacích, kde bezdrátová síť používá slabé šifrování!

„... Wireshark® is a network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network ...“

Man-In-The-Middle útoky

Snaha útočníka aktivně vstoupit např. do šifrovaného SSL spojení. Útočník má takto přístup k nešifrovaným datům.

Útočník předpokládá nedbalost uživatelů, kteří nevěnují pozornost kontrole dat v certifikátu.

Jiný příklad útoku na SSL z roku 2014 je chyba v označená jako HeartBleed

This is probably not the site you are looking for!

You attempted to reach **www.google.com**, but instead you actually reached a server identifying itself as ***.facebook.com**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **www.google.com**.

You cannot proceed because the website operator has requested heightened security for this domain.

Keyloggery

Nástroje pro zaznamenávání stisků na klávesnici – pokročilé keyloggery nabízí další funkčnosti – sledování schránky, pohybů myši.

Hardwarové keyloggery – fyzický přístup útočníka k zařízení

Upravená klávesnice, sledování elmg. vln, skryté kamery, ...

Softwarové keyloggery – instalace malware z nedůvěryhodných webů

Odesílání záznamů a jejich pozdější využití útočníkem

Sociálně-inženýrské metody získávání dat

Cílené spamové nebo phishingové kampaně

- Snaha vylákat z uživatele přístupové údaje nebo platby

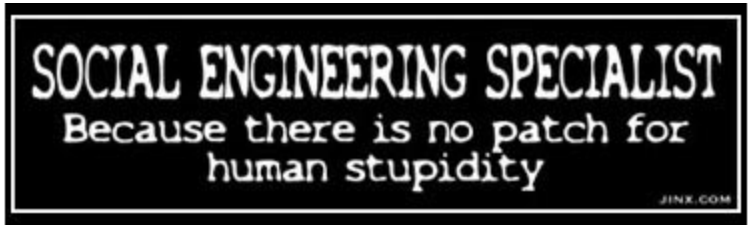
Spear-phishing

- Phishing z „důvěryhodného zdroje“ cílený na specifickou skupinu osob

Voice phishing

- Telefonát z call centra banky? Jak ověříme jeho pravost?

Whaling – cílem je např. skupina senior exekutivy



Prohlížeč – množství poskytnutých informací o uživateli

https://amiunique.org/

https://panopticlick.eff.org/

https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/

Doporučení:

- minimálně HTTPS Everywhere plugin
- vyzkoušet NoScript, Ghostery, zakázat JavaScript?

Krádež mobilních zařízení – nejslabší článek řetězu

Jaké informace máme v mobilním telefonu (tabletu, notebooku)?

Jak jsou tyto informace zabezpečené?

Jak často sebou zařízení máme každý den?

Jaká jsou rizika zneužití uložených informací v případě krádeže/ztrátě?

Zneužití osobních údajů v digitálním světě

Finanční motivace na prvním místě

- čísla kreditních karet
- přístupové údaje do ibankovnictví
- firemní know-how
- údaje o zákaznících
- údaje o zaměstnancích

Příklad úniku dat z obchodního řetězce Target v USA

- 40 milionů čísel kreditních karet
- 70 milionů záznamů o zákaznících
- 200 mil USD za vydání nových karet
- 100 mil USD za upgrade POS

Úniky osobních údajů

Většinou se dozvídáme ze zpráv, že se něco stalo, např.

Target eBay Google Facebook Seznam

nosiče s osobními údaji nalezené v popelnici

úniky osobních dat z trestních spisů

Stejně závažné jsou ale úniky směrem dovnitř organizací

špatně nastavená přístupová oprávnění zneužití pravomocí

V ČR je povinnost firem hlásit úniky osobních dat např. ČTÚ, ERU apod.

What the California Law Requires

California Civil Code section 1798 .29 applies to state government agencies and section 1798 .82 applies to businesses.

The statutes require any person or business that conducts business in California, and any state agency, that owns or licenses "**computerized data**" including personal information to notify any resident of California whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a breach of security.

The type of personal information that triggers the requirement to notify individuals is **unencrypted**, computerized information, consisting of an **individual's name**, plus one of the following: **Social Security number**; **driver's license or California Identification Card number**; **financial account number**, including **credit** or **debit** card number; **medical information** and **health insurance information**.

The 46 state breach notification laws are similar, because they are based on the California law.

Key Findings – California law

- In 2012 – 131 data breaches, each affecting more than 500 California residents
- The average (mean) incident involved the information of 22,500 individuals .
- More than 2.5 million Californians were put at risk by data breaches in 2012.
- More than 1.4 million Californians would not have been put at risk (28 percent of the data breaches), if the data had been encrypted.
- More than half of the breaches (56 percent) involved Social Security numbers, which pose the greatest risk of the most serious types of identity theft.
- More than half of the breaches (55 percent) were the result of intentional intrusions by outsiders or by unauthorized insiders. The other 45 percent were largely the result of failures to adopt or carry out appropriate security measures.
- Report: http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf

Zneužití přístupových údajů

Člověk je tvor pohodlný...

Pro řadu služeb na Internetu používá jedno nebo jen omezenou skupinu hesel

Jedno kompromitované heslo tak otevírá řadu přístupů

Kde všude hesla změnit? Jak zjistíme, že bylo heslo kompromitováno?

Co můžeme udělat pro minimalizaci rizik

Single-sign-on + silné heslo 2FA Použití správce hesel

Uvědomit si rizika spojená s kompromitováním našich přístupových údajů

Možnosti zneužití informací o poloze

Informace o poloze mobilního zařízení, které máme denně u sebe...

Pokud má útočník k dispozici geolokační informace z napadeného mobilu, má jistotu, že v dané oblasti jsme nebo naopak nikoliv.

Sdílení geolokace se servery na Internetu

Přibližné určení polohy podle IP adresy (na úrovni států, velkých měst)

http://www.iplocation.net/

Hodnota osobních informací na černém trhu

Čísla kreditních karet	$4 - $30	(v závislosti na typu, území platnosti)
Čísla bankovních účtů s přístupovými údaji	řádově stovky $	(v závislosti na zůstatku)
Datum narození	$10	
Kompromitované počítače	1000 počítačů za řádově desítky $	
Kompromitované účty na soc. sítích	1000 účtů za řádově desítky $	
Doxing	< $100 za osobu	

Pro zajímavost

DoS útok	$3-$5/hodina	$80-$100/den

http://securityaffairs.co/wordpress/19957/cyber-crime/cyber-criminal-underground.html

Doxing – document tracing

Sběr informací o konkrétní osobě

sociální sítě sdílený obsah

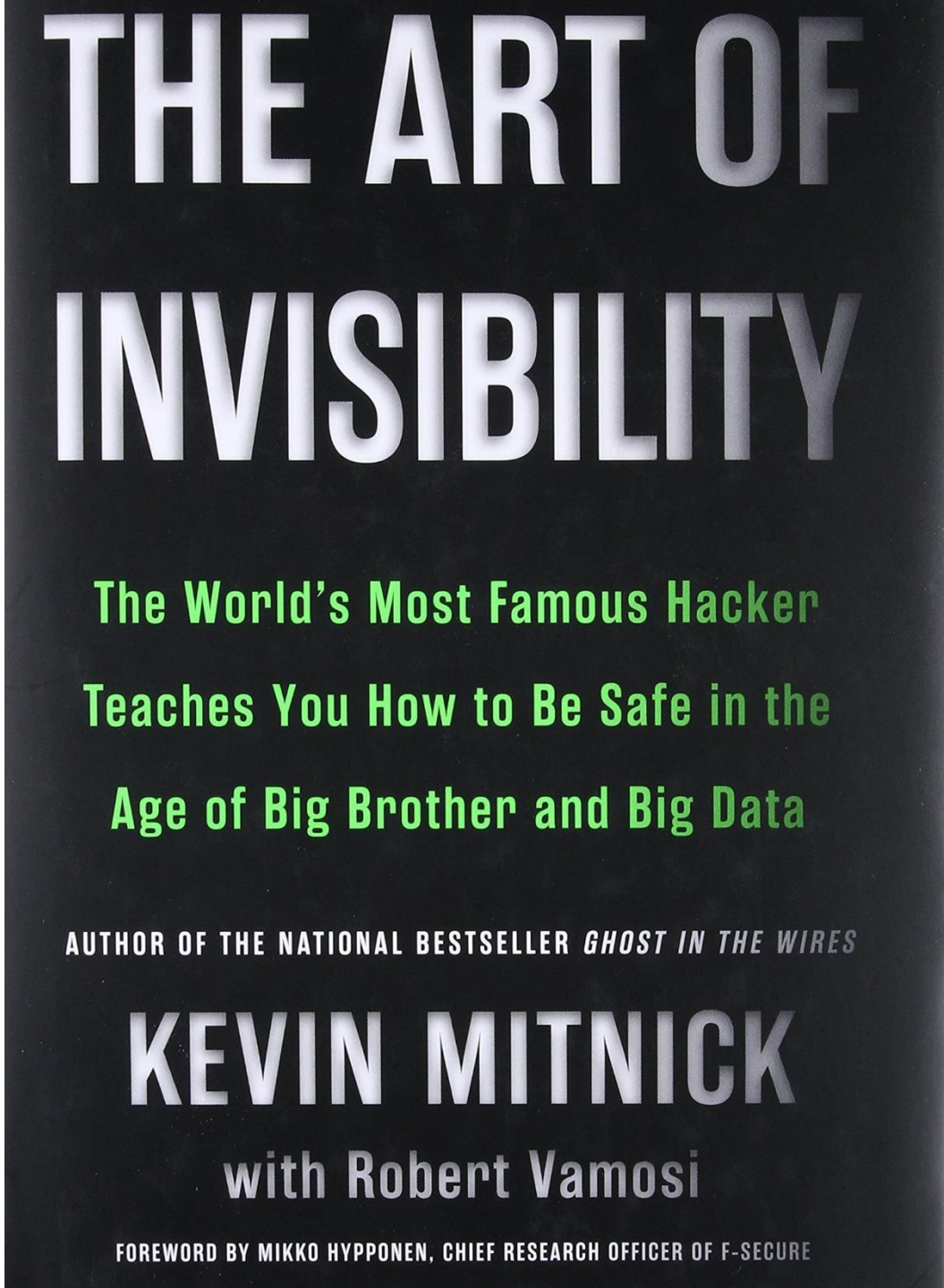
diskuzní fóra blogy

malware kompromitovaný počítač

kompromitovaná mobilní zařízení online hry

https://www.youtube.com/watch?v=F7pYHN9iC9I

Dotazy?


THE ART OF INVISIBILITY
The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data
AUTHOR OF THE NATIONAL BESTSELLER GHOST IN THE WIRES
KEVIN MITNICK
with Robert Vamosi
FOREWORD BY MIKKO HYPPONEN, CHIEF RESEARCH OFFICER OF F-SECURE