Chapter 1.4
Identity Theft Through the Web

Thomas M. Chen
Swansea University, UK

ABSTRACT

Most people recognize there are risks to online privacy but may not be fully aware of the various ways that personal information about them can be stolen through the Web. People can be lured to malicious Web sites designed to deceive them into revealing their personal information or unknowingly download malicious software to their computer. Even worse, legitimate sites can be compromised to host attacks called drive-by downloads. This chapter describes the online risks to identity theft and the technological means for protecting individuals from losing their personal information while surfing the Web.

INTRODUCTION

In the physical world, an individual's identity is verified by legal documents including passports, driver's licenses, birth certificates, and identification cards. Identity can also be authenticated by biological features (such as fingerprints or DNA) or demonstration of secret knowledge (passwords). Naturally, online identities can not rely on physical evidence. Instead, online identities are authenticated by personal information such as names, national identification or Social Security numbers, addresses, driver's license numbers, telephone numbers, account numbers, credit card numbers, and passwords or PIN numbers (Berghel, 2000).

Generally, identity theft is the gain of an individual's personal information for fraudulent purposes. In the U.S., the Identity Theft and Assumption Deterrence Act of 1998 was the first federal law to explicitly make identity theft a federal crime. An individual commits identity theft when the person:

"knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation

DOI: 10.4018/978-1-61350-323-2.ch1.4

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

of Federal law, or that constitutes a felony under any applicable State or local law"

The law recognized that individuals affected by identity theft are victims, where previously only credit organizations suffering financial losses were seen as victims. The law made it easier to prosecute perpetrators with penalties up to 15 years imprisonment and fines up to $250,000. As a federal crime, identity theft is investigated by the Secret Service, the Federal Bureau of Investigation, and other law enforcement agencies. The Federal Trade Commission was enlisted as a clearinghouse for complaints and assistance for victims.

Millions of consumers in the U.S. are affected each year, costing consumers and businesses tens of billions of dollars, according to the Federal Trade Commission. On average, a victim resolves a fraud at a personal cost of $500-1,400 and over 30 hours of time. Identity theft can be even more costly to businesses. In addition to fraudulent charges, businesses could be subject to legal complications for lack of compliance with laws and regulations. The Gramm-Leach-Bliley Act requires all financial organizations to have appropriate security standards to protect customer information. The Fair and Accurate Credit Transaction Act (FACTA) of 2003 is an amendment of the Fair Credit Reporting Act placing responsibility on corporations to protect personal customer and employee information at a risk of state fines up to $1,000 per violation and a federal fine up to $2,500 per violation.

There have been many low-tech ways for criminals to steal personal information, for example, dumpster diving, mail theft, court records, computer (particularly laptop) theft, cell phone theft, and social engineering. Social engineering scams take advantage of human nature to deceive victims. A caller might claim to be an employee at your credit card company checking on your account for suspicious transactions; in the process, you need to verify your personal details.

However, the World Wide Web offers another convenient avenue to steal personal data in a number of ways. First, web servers holding personal account data are attractive targets to attackers and can be attacked like any other computer system. In particular, web servers with back end databases may be vulnerable to SQL injection attacks. Second, the web has enabled phishing attacks luring consumers into disclosing their personal information on spoofed web sites. Third, the web is being used as a vector to distribute various forms of malicious software (malware), including viruses, spyware, bots, and Trojan horses.

This chapter describes the unlawful theft of personal information through the web, focusing on phishing, drive-by downloading, and SQL injection. These are common theft techniques but certainly not the only ones. We do not cover more general Internet-related identity theft, such as sniffing (eavesdropping on packets), password cracking (gaining access to servers by guessing passwords), or malware delivered through e-mail. There are many ways to steal data through the Internet that are not related the web and hence not covered here. Also, we do not cover the subsequent criminal use of that stolen information, e.g., to steal money, make illegal purchases, hijack accounts, or open new accounts.

Review of Web Technologies

The web uses a client-server architecture as shown in Figure 1. HTML (hypertext markup language) pages are stored on web servers which wait for requests from web clients (browsers). Web documents are identified by URLs (uniform resource locators) with the well known format such as http://www.domain.com/a/b/index.html indicating the path to the document index.html located on the server at www.domain.com. The domain is resolved to an IP address by a query to DNS (domain name system). The application layer protocol between clients and servers is HTTP (hypertext transfer protocol), which uses

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/identity-theft-through-web/60940

Related Content

A Cloud-User Watermarking Protocol Protecting the Right to Be Forgotten for the Outsourced Plain Images
Xiaojuan Dong, Weiming Zhang, Xianjun Huand Keyang Liu (2018). *International Journal of Digital Crime and Forensics (pp. 118-139).*
www.irma-international.org/article/a-cloud-user-watermarking-protocol-protecting-the-right-to-be-forgotten-for-the-outsourced-plain-images/210141

A Framework for Privacy Assurance and Ubiquitous Knowledge Discovery in Health 2.0 Data Mashups
Jun Huand Liam Peyton (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 263-283).*
www.irma-international.org/chapter/framework-privacy-assurance-ubiquitous-knowledge/60953

The Human Factor in Mobile Phishing
Rasha Salah El-Din, Paul Cairnsand John Clark (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism (pp. 53-65).*
www.irma-international.org/chapter/the-human-factor-in-mobile-phishing/131397

An Image Region Description Method Based on Step Sector Statistics and its Application in Image Copy-Rotate/Flip-Move Forgery Detection
Likai Chen, Wei Luand Jiangqun Ni (2013). *Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security (pp. 35-49).*
www.irma-international.org/chapter/image-region-description-method-based/75662

Reversible Watermarking on Stereo Audio Signals by Exploring Inter-Channel Correlation
Yuanxin Wu, Wen Diao, Dongdong Houand Weiming Zhang (2019). *International Journal of Digital Crime and Forensics (pp. 29-45).*
www.irma-international.org/article/reversible-watermarking-on-stereo-audio-signals-by-exploring-inter-channel-correlation/215320