COSC130

Fundamentals of Cybersecurity and Privacy

LECTURE 6: HOW TO PROTECT YOURSELF ONLINE – INTRODUCTION + AUTHENTICATION

How to Protect Yourself Online
Introduction and Authentication

1. Introduction
2. Case Studies
   - Sony's PlayStation network Attack 2012
   - Abode Systems Attack 2013
3. Authentication
   - Passwords
   - Two-Factor Authentication

Much of this lecture is based on

OpenLearn. *Introduction to Cyber Security*, 2016.

In-text references to this source are typically omitted for readability.

Introduction to Cybersecurity

In recent times, many things that we can do in the physical world, we can also do online:

1. Working and studying: attending classes, attending meetings,
2. Healthcare: doctor’s appointments, getting prescriptions, ordering medication, medical claims
3. Staying connected: socialising, playing games, sending and receiving messages, audio and/or video chats
4. Everyday life: shopping, ordering food, banking, paying bills, tax returns, insurance claims

Then it is no surprise to anyone that we now have a new type pf criminals operating in the cyberspace – cybercriminals (typically referred to as ‘attackers’ in cybersecurity).

Introduction to Cybersecurity

How common is cybercrime?

Recall that in 2021-2022 financial year, 76,000 cybercrimes were reported in Australia – that is, on average, around 9 cybercrimes per hour.

However, we know that only a small proportion of cybercrimes gets reported – the real numbers are much bigger.

Who has a responsibility to protect against cybercrimes?

We all do!

How can we do that?

We can do that by:

1. Staying vigilant
2. Protecting our own data and other resources
3. Reporting crimes and suspicions activities

Case Study: 2011 Sony's PlayStation Network Attack

What Happened?

In April 2011, PlayStation Network was breached and around 70,000,000 customer records were stolen. They included names, addresses, emails, dates of births and account password details.

What security service(s) were breached? For you to answer ☺

What did Sony do?

Sony took the PlayStation Network off-line to assess the damage and patch the vulnerabilities that enabled the attack.

How much did it cost them?

The cost to Sony was estimated to be 105,000,000 pounds. This includes

1) loss of revenue while the network was offline
2) 250,000 pounds fine for serious breach of the Data Protection

but it does not include

1) loss of revenue by the partner companies (e.g., those who advertise on the PlayStation Network)
2) loss of Sony's reputation
3) cost of PlayStation customers (e.g., possible identity theft, etc.)

Case Study: 2013 Adobe Systems Attack

What Happened?

On the 3rd Oct 2013, Adobe Systems reported that between 30 Aug and 17 Sep 2013, 'an unauthorised third party illegally accessed certain customer order information'. It slowly transpired that the attacker compromised a web server and used it to access another server that hosted a back up database containing the following information about over 153,000,000 customers world-wide. All the information was in unencrypted format (plain-text) unless stated otherwise.

1) Adobe usernames
2) names
3) email addresses
4) addresses and phone number of some users
5) encrypted passwords (and possibly some unencrypted passwords stored in a separate database)
6) encrypted credit card numbers

The attacker stole a copy of the database, and it eventually became widely available on the internet.

What security service(s) were breached? For you to answer ☺

Case Study: 2013 Adobe Systems Attack

What did Adobe do?

Adobe Systems did the following to contain and rectify the breach:

1) disconnected the compromised server from the network
2) started an investigation
3) blacklisted attacker's IP addresses
4) changed passwords for all administrator accounts
5) changed passwords for all affected users
6) notified affected users expressing regret for the inconvenience
7) notified affected banks
8) notified low enforcement agencies
9) sent takedown requests to operators of the servers hosting the stolen data

Case Study: 2013 Adobe Systems Attack

What did Law Enforcement agencies do?

Among the affected users, there were around 2,000,000 Australians, which led the Australian Privacy Commissioner to instigate its own investigation in which they considered the following:

1) Privacy Act 1988

2) Particular circumstances

3) Adobe's submission

4) information collected from other sources, including results of data breach analysis conducted by the Data Protection Commissioner of Ireland and the Office of Privacy Commissioner of Canada.

Case Study: 2013 Adobe Systems Attack

Relevant Provisions of the Privacy Act 1988

The Australian Privacy Principles (APP) that we discussed came into power on the 12 Mar 20914. Before that, there were ten National Privacy Principles (NPP) that organization covered by then Act had to comply with.

The relevant NPPs were NPP 2 and NPP 4.1.

1) NPP 2 states that 'an organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection, unless a listed exception applies'.

2) NPP 4.1 states that 'an organization must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification, or disclosure'.

Case Study: 2013 Adobe Systems Attack

Particular circumstances

Particular circumstances included the following:

1) the amount of personal information
2) the sensitivity of the information
3) the risk to the affected individuals
4) how easy or hard was for Adobe Systems to implement security measures to protect personal information.

Organisations are expected to implement a range of security safeguards to protect personal information from relevant security threats.

Case Study: 2013 Adobe Systems Attack

Adobe's submission

At the time of the data breach, Adobe Systems had a range of security measures in place, including the following:

1) firewalls, two-factor authentication for remote access, web traffic filtering and antimalware software
2) all Abode employees had access to security training material and IT specialists had an annual security training
3) intrusion detection and prevention system, traffic monitoring
4) annual audit of the server hosting the stolen database
5) incidence response plans
6) risk assessment programs

Case Study: 2013 Adobe Systems Attack

The stolen database was a backup that was scheduled to be decommissioned but was still in use at the time of the attack. It stored

1) Usernames
2) Email Addresses
3) Encrypted passwords and credit card numbers, using a single encryption key
4) Password hints in plaintext – some of the were obvious hints or even passwords themselves

Case Study: 2013 Adobe Systems Attack

Findings

The Australian Privacy Commissioner found that Adobe Systems did not breached NPP 2 but breached NPP 4.1 by failing to 'take reasonable steps to protect all of the personal information it held from misuse and loss and from unauthorized access, modification or disclosure'.

For more information, see "Adobe Systems Software Ireland Ltd: own motion investigation report" at https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/investigation-reports/adobe-systems-software-ireland-ltd-own-motion-investigation-report

What can we learn from these case studies?

Lesson 1

Murphy’s law – if something can go wrong, it will!

Lesson 2

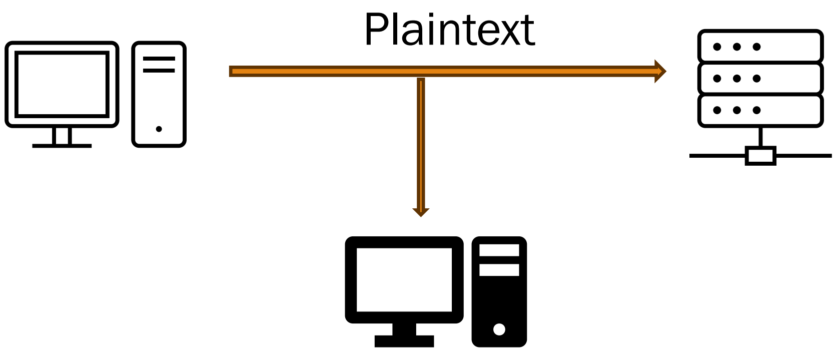
Once somebody has our information (e.g., your credit card number), we depend on them to protect it.

Lesson 2

In the Abode System data breach, we saw that weak passwords were much more vulnerable than strong ones.
It is very important that we choose strong passwords!!!

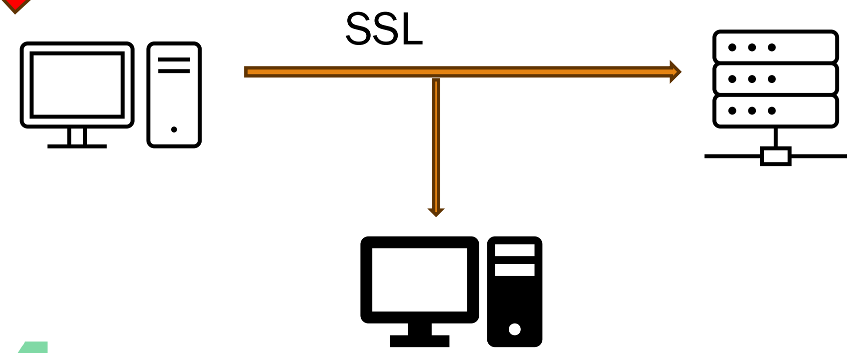
Authentication and Passwords

Version 1 ✗



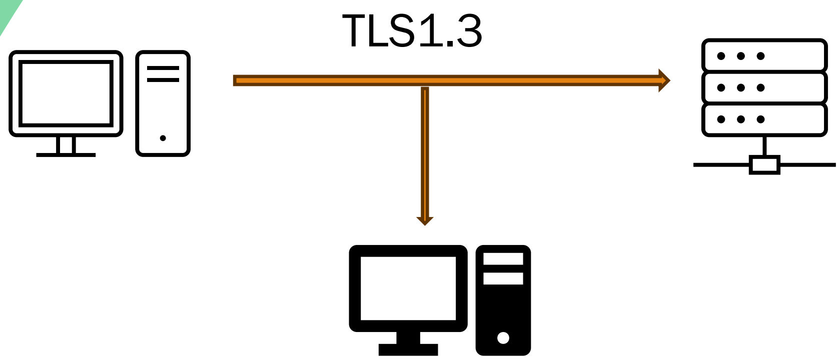
Name	Password (Plaintext)
John	letmein
Mary	letmein
…	…

Version 2 ✗



Name	Password (Encrypted)
John	ghnuy
Mary	ghnuy
…	…

Version 3 ✓



Name	Password (Hashed)	Salt
John	bcuiw7Yj	xvw78bn@3
Mary	mSNbe%w7	Nma7%6vb
…	…	

Authentication and Passwords

Summary:

1) **Encryption** converts plaintext into cyphertext using a secret key. This process is reversible – ciphertext can be decrypted to recover the plaintext.

2) **Hashing** converts plaintext into a hash code without using a key. This process is not reversible, and it is computationally infeasible to recover the plaintext from the hash code.

3) Salting is a process of adding a random sequence of characters to a password before hashing.

4) If passwords are encrypted, then the same ciphertext means that the passwords are also the same.

5) If unique salt is used for each password, then hashed values will be different, even if passwords are the same.

Attacks on Passwords

Looking over somebody's shoulder

Very weak passwords

Dictionary words, name of a spouse, '12345', etc

Dictionary Attack

Trying all passwords from a dictionary containing not only valid words and phrases but also all compromised passwords, names, etc

Brute Force Attack

Trying all possible combinations of characters

Generating Strong Passwords

Tips for generating strong passwords

1) The best passwords are random sequences of lower- and upper-case letters, numbers, and special characters, at least 12 characters long but preferably even longer.

2) As such passwords are hard to remember, you may think of a sentence that is meaningful to you, and use just the first letter from each word, capitalize some of the letters, and insert some numbers and special characters. Such passwords are easy to remember but hard to crack.

3) Don’t use the same passwords for different purposes

Password Management

Password managers are software applications that can

1) store different passwords
2) generate strong passwords.

A good password manager will

1) require you to use a password to access it
2) lock out after a period of inactivity
3) store your passwords in encrypted form (either on your computer or on the cloud)

Password Management

Pros

1) You can use strong passwords without needing to remember them – you only need to remember one strong password for the password manager itself.
2) Password managers are usually convenient to use.

Cons

1) Password managers represent the so-called ‘single point of failure’ as compromising your password manager allows attackers to learn all your passwords. It comes as no surprise that password managers are a prime target for attackers.
2) If, for any reason, you don’t have access to your password manager, you don’t have access to any of your passwords.

Two-Factor Authentication

Two-factor authentication is a system where you have to provide two pieces of information (or physical objects) to authenticate yourself, rather than just a password.

For example, to withdraw money from an ATM, you need to provide both your bank card and your pin.

Similarly, when you pay using your bank card, you typically need to swipe or tap your card, and provide your pin.

Which one of the following is a two-factor authentication?

1) Security Service
2) Security Mechanism
3) Security Attack
4) Security Vulnerability

Two-Factor Authentication

Which one of the following types of security mechanisms does the two-factor authentication belong to?

Proactive:

- Preventive controls
- Deterrence
- Deflection

Reactive approaches:

- Detection
- Mitigation
- Recovery

Two-Factor Authentication

Today many websites, including online banking systems support two-factor authentication.

When you try to log in, the website sends an SMS to your phone with a unique code that you then need to enter on the website in order to log in.

Alternatively, you can install an authenticator app on your phone or computer, for example, Duo Mobile.

This will of course not work if an attacker steals your phone and finds out your phone pin.

References

[**OpenLern, 2016**] OpenLearn. *Introduction to Cyber Security*, *2016*.

[**OAIC, 2015**] Office of Australian Information Commissioner, “Adobe Systems Software Ireland Ltd: own motion investigation report”, 2015.