Common Threats and Solutions

For the Average Citizen

Irfan Kanat

Department of Digitization
Copenhagen Business School

May 24, 2021

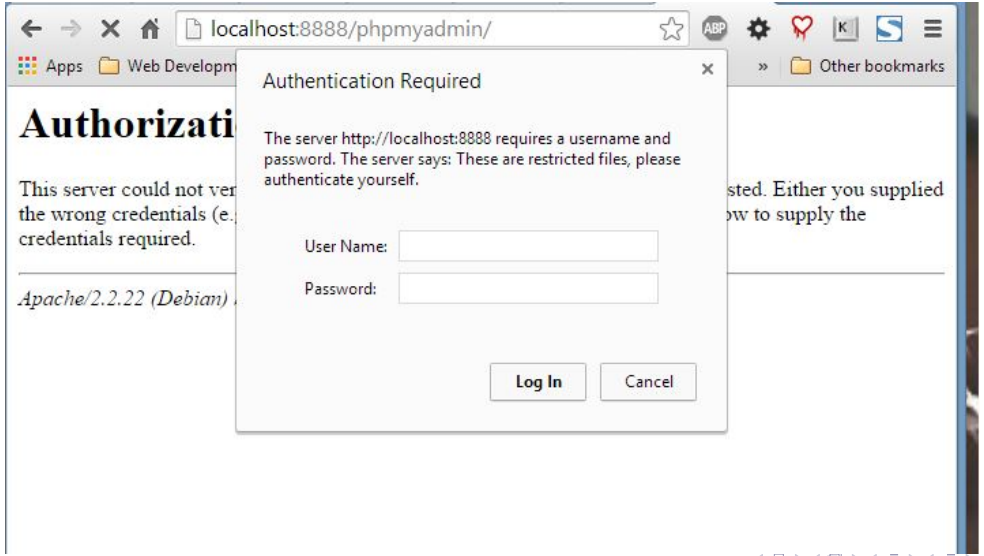
In the previous modules we learned about privacy, stalking, and surveillance as well as reducing your foot print online to make tracking harder. In this module we will learn about typical threats facing an average citizen and how to improve your security against them. In the previous module our focus was on the network traffic, now our focus will be on device security.

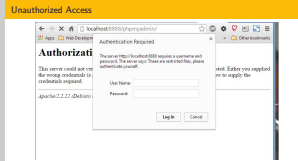
Common Threats

- Unauthorized Access
- Bugs
- Malware
- Network Access

Common Threats
- Unauthorized Access
- Bugs
- Malware
- Network Access

Unauthorized Access





This is essentially an adversary gaining access to resources they shouldn't have access to. While the topic of unauthorized access is much broader, for a typical citizen in his/her private life it often comes down to authentication.

Authentication today is mostly done through passwords. Just like it was 40 years ago. It is hard to believe, but we haven't been able to find a better way...

The adversary can be someone you know, or a malicious third party.

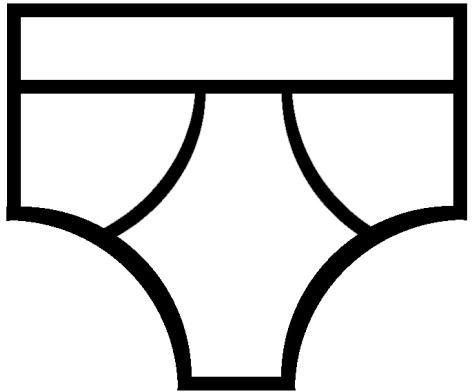
The way they gain access can be either by guessing your password, trying random passwords until they find the one, tricking you into sharing your password, or using a password you used elsewhere.

Passwords are like Underwear

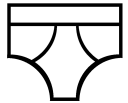
Don't leave them lying around.

Don't share them with others.

Change them often.

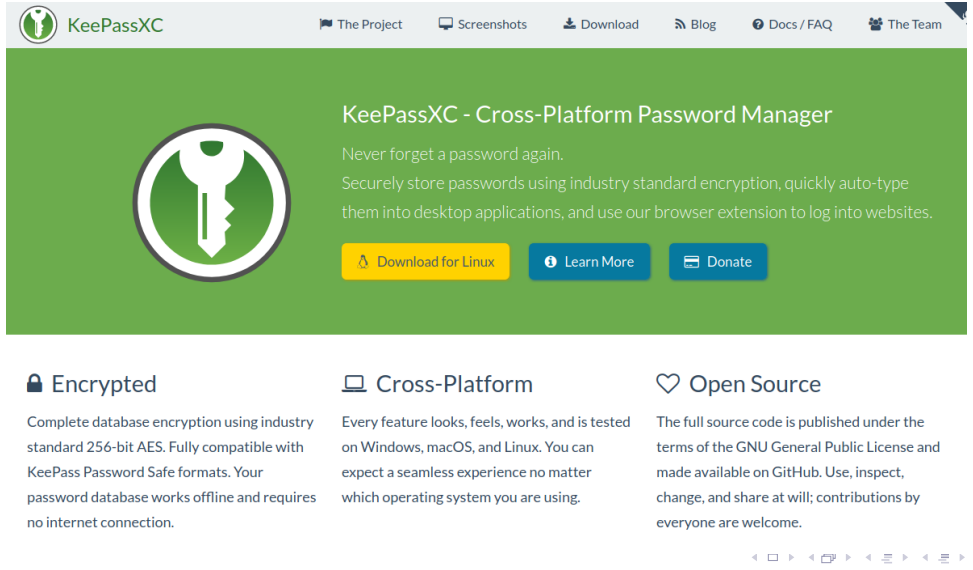


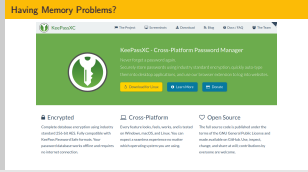
Passwords are like Underwear
Don't leave them lying around.
Don't share them with others.
Change them often.



Long story short, treat password like you would treat your underwear.
Don't write it down.
Don't tell it to others.
Don't reuse it in many places.
Don't pick something that is easy to guess.
Don't pick meaningful words...

Having Memory Problems?





Multi Factor Authentication

- Something You Know
- Something You Are
- Something You Have

Multi Factor Authentication
Something You Know
Something You Are
Something You Have

A strong password may be hard to remember...
If you follow good advice and use a different password for every site, then that means you need to remember dozens of hard to remember passwords that are not easy to remember...
Solution is to store your passwords in an encrypted repository.
There are some cloud based solutions, but like with everything else, it comes down to trust. Recently a cloud based provider began charging users for access. When that happens, a password manager can be like ransomware.
Therefore I recommend using open source software. You the user will be in control of where your passwords are stored.

Bugs

Natural

Sometimes can be exploited

Bugs
Natural
Sometimes can be exploited

Modern software can run into millions of lines of code... The size of the modern software, combined with all the parts that interact with each other make it a very complex endeavor. Akin to designing a jumbo jet...

This means programmers make mistakes in the code. Some of these won't ever be noticed. Some of the ones we notice, may not harm the daily operation of the system... Others can be used for malicious purposes.

In worst cases bugs can be used to escalate privilages, meaning the adversary can bypass controls and gain control of the device.

Update All Software All the Time

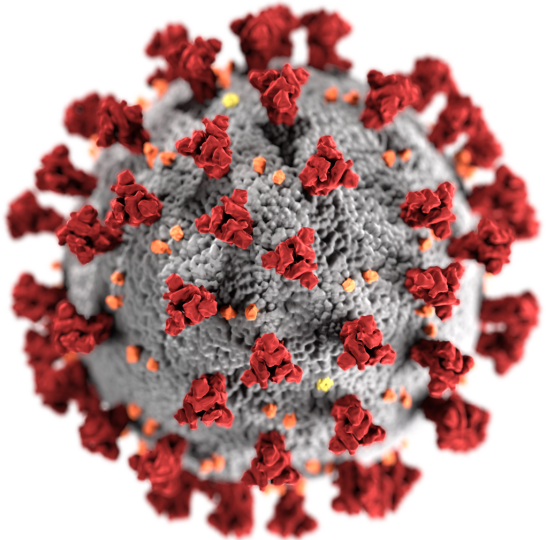
- Update your software regularly.
- All of it
  - Operating System
  - Applications
  - Firmware

Update All Software All the Time
- Update your software regularly.
- All of it
  - Operating System
  - Applications
  - Firmware

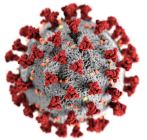
Developers release updates to their software that fixes these bugs.
Once a bug is known, it is easy pickings for attackers.
Therefore it is imperative you keep your system up to date.
One thing you need to know is to stop using hardware and software that no longer receives security updates. This applies to everything: operating systems, applications, cell phones...

Malware

- Viruses
- Trojans
- Worms
- Ransomware
- Rootkits



Malware
- Viruses
- Trojans
- Worms
- Ransomware
- Rootkits



Besides innocent mistakes, there is software written with malicious intent.
Worst of this can spread without user interaction, like NotPetya worm.
But most of it requires user to click a link, open a document, run a program...

Against Malware

- Update your system.
- Update your anti-virus software.
- Regularly scan your system.
- Don't open files you don't know.

Against Malware
- Update your system.
- Update your anti-virus software.
- Regularly scan your system.
- Don't open files you don't know.

Malware can spread exploiting bugs in your software. Updating your software can protect you against getting infected.

Anti-virus software can identify and stop known malware. It is important to update virus definitions in your anti-virus software to know your defenses are up to date.

Most importantly, be careful what you click on. Many web sites on the internet are full of malicious links. As a rule of thumb, don't click or run anything you are unsure about.

In fact it is often office policy these days to not include or click on any links in any e-mails.

If a friend for example sent you a file without explanation, ask him what it is through another channel. So if he sent you a file in an e-mail, ask about it over the phone. To make sure it is indeed a legitimate file sent to you.

Network Access

Open Ports + Bugs = Trouble

Network Access
Open Ports + Bugs = Trouble

Software communicate through ports. Imagine this as your computer having many doors to the internet and a program listening, waiting behind each of them.

Your web browser is using a door, your e-mail client is using another, software updates come and go through yet another. Even Tiktok gets a door of its own.

You often won't even realize the software you install opens up a new port (door) to your computer.

A piece of malware, or a malicious actor can exploit the bugs in the software behind open ports to gain access to your device. So a combination of open ports and buggy software often creates trouble.

As with any defensive scenario, the more openings you need to watch, the poorer your security.

Therefore it is important to keep track of these doors.

Firewalls

Firewalls

Despite the cool name, what a firewall does is more akin to a border control agent.
A firewall is a set of rules that define the admissable traffic for a device.
What port, what protocol, which direction, from where?
Denying traffic on ports you don't use or recognize can save you trouble down the road. The problem is, you may accidentally block legitimate traffic if you are not careful...

In Short

- Use Strong Passwords
- Don't Engage if You Didn't Initiate
- Update Your Software
- Remove Unnecessary Software from Your Life
- Use Anti-Virus
- Setup a Firewall

In Short
- Use Strong Passwords
- Don't Engage if You Didn't Initiate
- Update Your Software
- Remove Unnecessary Software from Your Life
- Use Anti-Virus
- Setup a Firewall