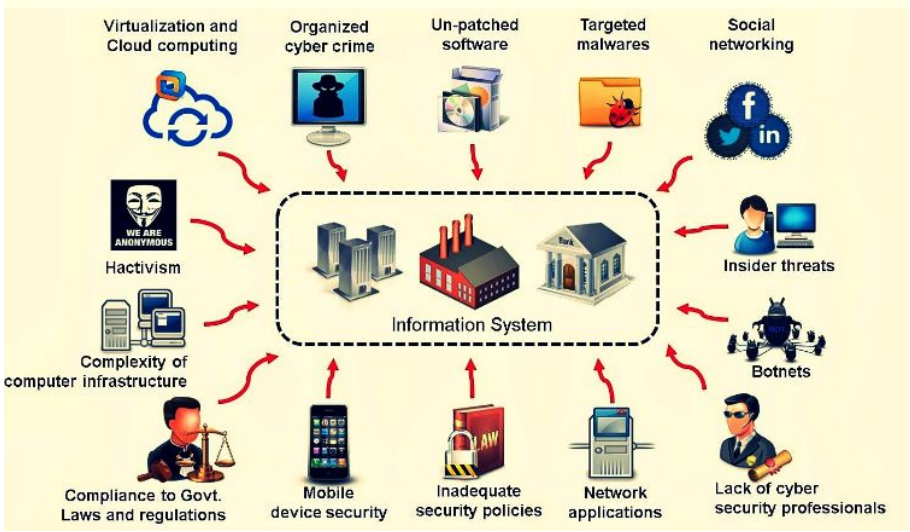
Topics in Security

Cybersecurity is HUGE

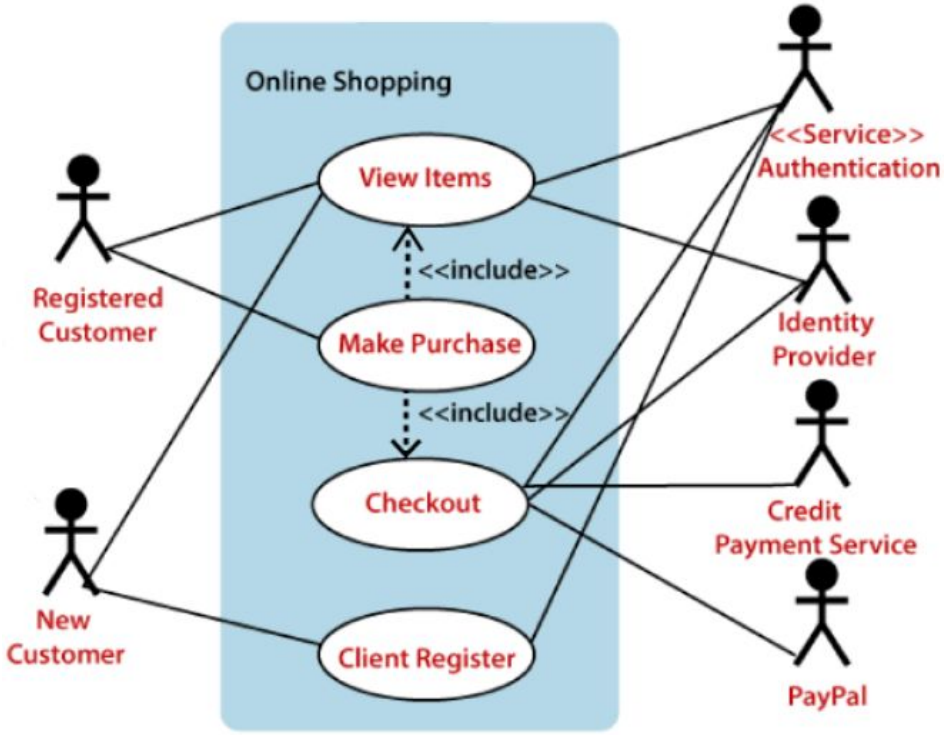


4 Topics to Discuss

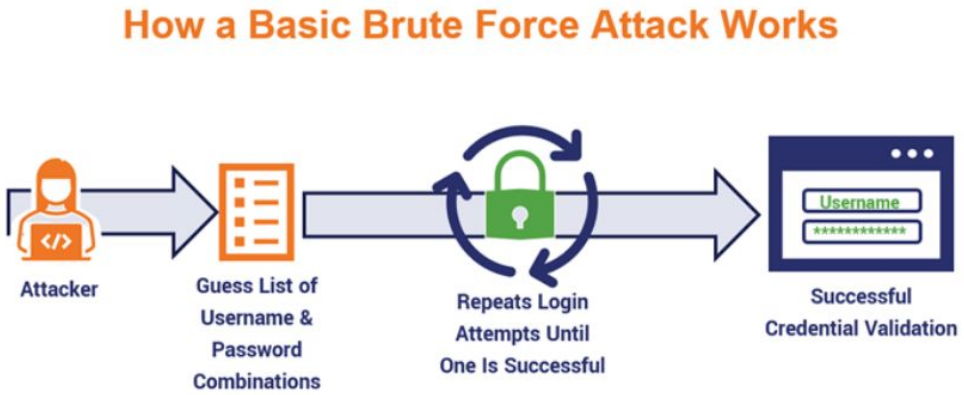
- Access Control
  - E.g.: Passwords, Permissions, Privileges, etc.
- Malware
  - E.g.: Ransomware, Spyware (Keyloggers), Rootkits, etc.
- Man-in-the-Middle
  - E.g.: Session Hijacking, Active Eavesdropping, etc.
- Social Engineering
  - E.g.: Phishing, Baiting, etc.

Access Control

- Only certain users/entities are allowed to perform certain actions or access certain data
- Need to **control access** to those actions and data based
- Must define what users/entities are allowed to do in the system (can be done many different ways)
- An attacker tries to gain access to things they shouldn't be able to do/see in the system



Access Control: How the Attack Works



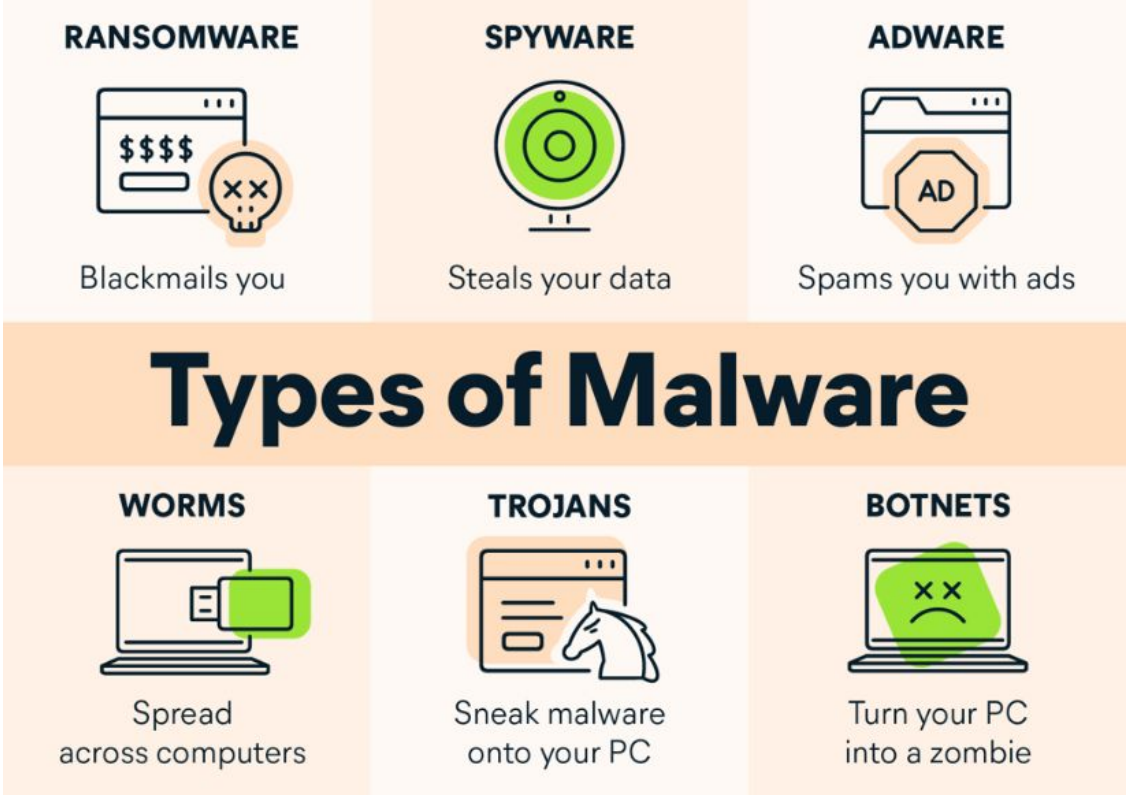
- Many different versions of the Brute Force Attack
  - Password Spraying
  - Dictionary Attack
  - Credentials Stuffing

Access Control: How Do We Stop It?

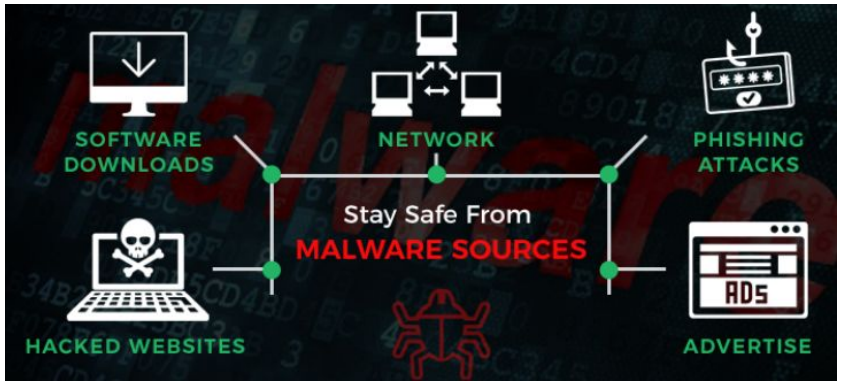
- Password requirements
- Maximum login attempts
- Proper validation and sanitization of user input
- Proper, well-derived, sophisticated access and permission policies

Malware

- MANY different types of malware and different types of attacks
- The common theme is that an attacker was able to execute or save some of their code on your computer



Malware: How the Attack Works



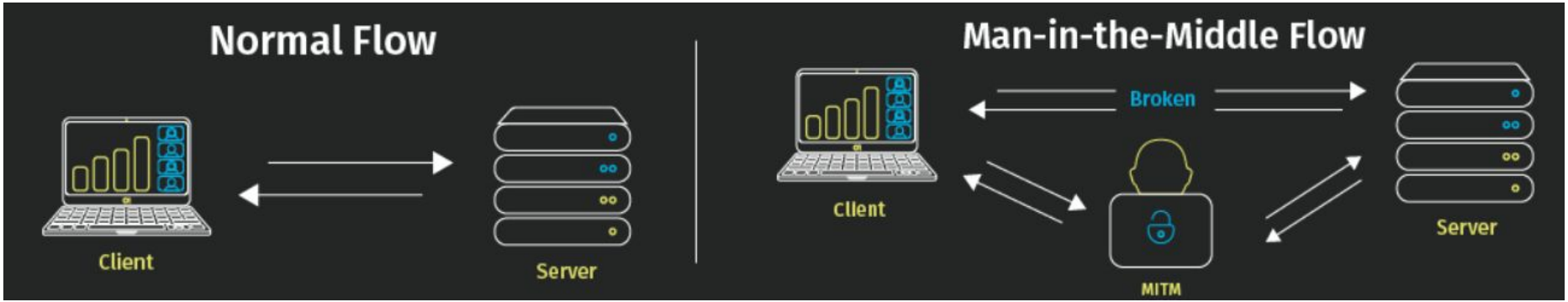
- Gets the user to download, install, open, enable, or otherwise run code that will do some kind of harm to your computer or data

- Can come from:
  - software packages
  - files, websites, and email with scripting and macros
  - removable storage devices that you were given or found
  - and more

Malware: How Do We Stop It?

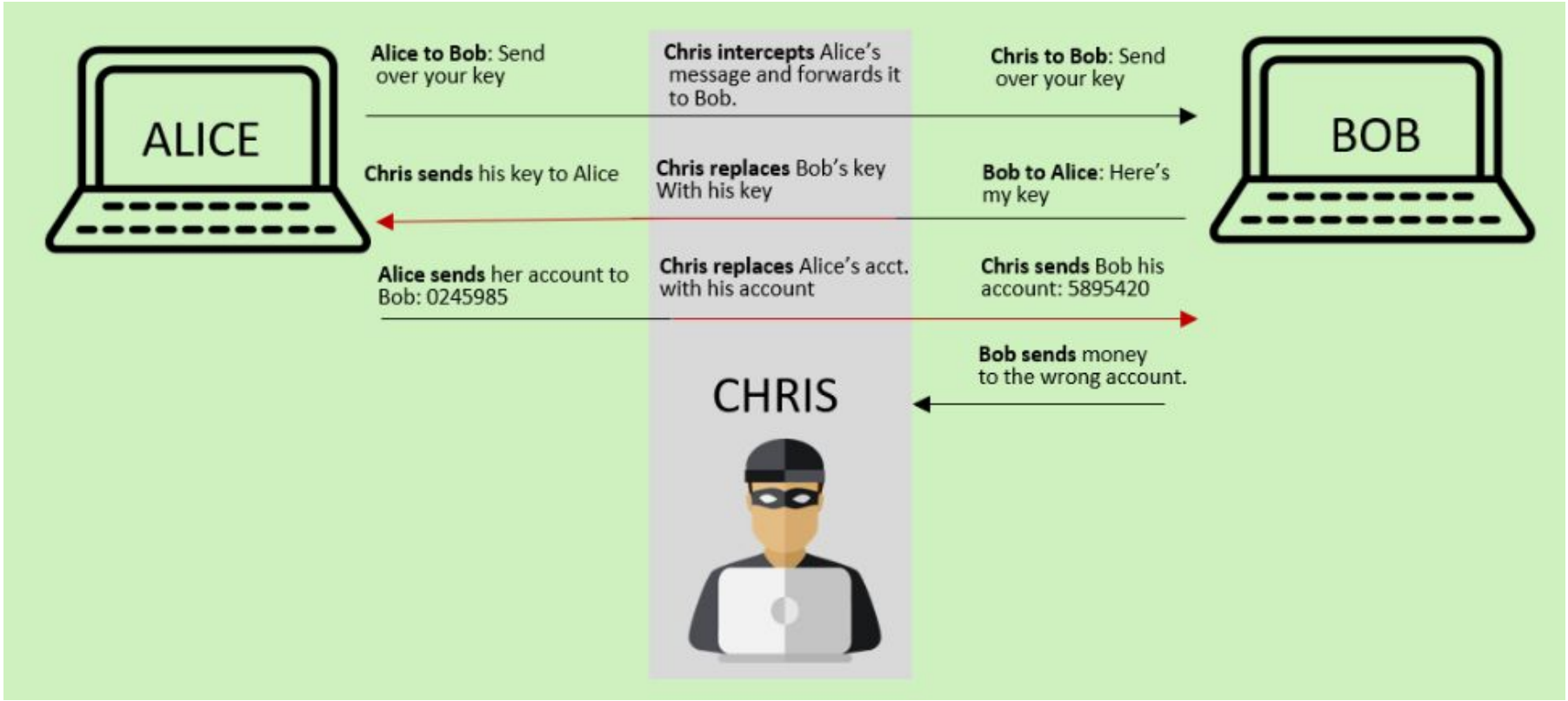
- Backup your computer often
- Be careful of sites you visit, attachments you download/open, and software you install
- Antivirus software
- Website certificates
- Email filters and alerts

Man-in-the-Middle



- Interrupt/Hijack the “normal” connection and insert themselves so your connection MUST go through them
- They receive the communication first, do whatever they want to it, then send it on its way

Man-in-the-Middle: How the Attack Works



Man-in-the-Middle: How Do We Stop It?

- There is little one can do once the attacker has successfully become the man in the middle

- Need to prevent the attacker from being able to be in the middle in the first place
  - Using HTTPS
  - Virtual Private Networks (VPNs)
  - Public key encryption

Social Engineering

- The least “technical” of the attacks
- A person tricks you into giving them sensitive data (essentially, a scam but in digital form or for digital data/access)
- Most “en masse” attacks are easy to detect, but highly specialized and sophisticated attacks can sometimes be very difficult to identify

Social Engineering: How the Attack Works

- Phishing
  - Use messages to gain a person’s trust
  - Once trusted, the person is asked for specific sensitive information (like a username and password) to then gain access to system under the name of that person

- Baiting
  - Usually involves coaxing a person to use some information or device that has been planted by an attacker

Social Engineering: How Do We Stop It?

- Email filters and tagging
- User knowledge and training
  - Never give out credentials
  - Never use something that isn’t yours (or, at least, don’t let it interact with any of your other devices)
- Browser filters

Attacks Do Not Exist in a Vacuum

- While sometimes attackers will simply try one type of attack at a time, it is a bit rare

- Using many types of attacks at once or switching tactics to gain more and more control of a system or network is common