Dave Sizer

10/31/16

CS472 HW3 Questions

1. FTP is inherently insecure, but this is because it simply was not designed with security in mind. It's an old protocol, from a time when the internet was a lot smaller and therefore when security considerations weren't as important. It simply sends all control information as plaintext strings, and has little or no consideration for authentication, which is also done in plaintext. BitTorrent, similarly, is not designed for security, but for speed. All communication goes through an unencrypted http connection to the tracker, and peer-peer connections are not authenticated. In both of these cases, the lack of security is by design, not due to a bad implementation, although a bad implementation could certainly make it even worse.
2. Absolutely. You could go in the "front door" by packet sniffing the user and pass commands, and using these credentials to log in. You could also through a similar technique intercept a data connection after PASV is initiated, for example.
3. A main security consideration that I implemented on my server was limiting users of the server only to the root directory of the server and lower, so that they only have access to pre-determined parts of the file system. You also would have to be very weary about executing anything uploaded to an FTP server, like anything you download from the internet. Also note that files are transmitted unencrypted, so they could be sniffed as well.