Part One

1. 1/259 Emails is malicious, Malicious && Malicious - 98/100, Non-Malicious && Non-Malicious - 98/100

   Using Bayes Theorem:
   Let s = “Safe email”,
   + = “A positive test for malware”

   P(s|+) = P(+|s) P(s) / P(+)

   = (2/100)(258/259) / ((258/259)(2/100) + (1/259)(98/100))
   = (129/6475) / (307/12950)
   = 113 / 2590
   = 0.043
   = 4.3%

   Bayes Theorem calculates that the possibility of an email being safe based on it having tested positive for malware is equal to 4.3%.
   [https://www.youtube.com/watch?v=j2tNxIaGpR4]

2. MessageDigest.isEqual compares two digests (byte arrays) for equality. This is vulnerable to a timing attack because it uses a variable time algorithm to compare the two digests instead of a fixed time algorithm. It will therefore take longer to run for each correct byte going from left to right.
   [http://codahale.com/a-lesson-in-timing-attacks/]

3. A salami attack is when a many small attacks sum up to equal a single large attack. The intent behind breaking up the attacks is to go unnoticed as small amounts by themselves creates less alarm than a larger amount. An example of this is in 2008 when a man was arrested for fraudulently creating 58,000 accounts which he used to collect money through verification deposits from online brokerage firms a few cents at a time.
   [http://en.wikipedia.org/wiki/Salami_slicing]

4. BHO’s (Browser Helper Objects) are basically an earlier version of browser plugins. They allowed the user to add functionality to their browser such as reading PDF files etc. These can be used maliciously as they have access to the browsers event model and can therefore be used to track the users actions within the browser such as accessing a secure financial institution. It would then record their keystrokes and transmit it to a malicious website for criminal use.
   [http://en.wikipedia.org/wiki/Browser_Helper_Object]

5. Buffer underruns are a state occurring when a buffer fed at a lower speed than it is reading from. This requires the program to pause processing while the buffer refills. This can cause the system to fail and allow blockages for extended periods of time. An example of a buffer underrun is the buffer for a graphics controller, if the system stalls this will cause the picture displayed to hang until the buffer receives new data. [http://en.wikipedia.org/wiki/Buffer_underrun]

6. A honeypot can be used to aid spam filters on “real systems” creating an action for the client to complete that would normally not be completed by a human we can add an additional metric to further distinguish humans from machines. An example of this is on web forms, by hiding a textfield using CSS it becomes very unlikely that a human will be able to fill out that field as they will need to disable CSS to fill it, a machine however is unlikely to use CSS and will fill out the form input automatically. If this input is filled it can be used to tell if a message is spam.

7.

- Online games that require email, passwords, security questions or credit card details create the risk of that information being stolen and your information being used to commit fraud.
    - Example: Blizzard suffered a major breach when their battle.net service was compromised giving out thousands of players emails, security question answers and two-factor authentication information. [1]
- Online games that use non-verified third party servers allow a compromised or malicious server to also compromise any computers that connect to it. Exploiting vulnerabilities within the users system or the game client may lead to malicious software being installed on the users system, gaining control of the users machine or getting information from the users machine.
    - Example: Games such as Age of Conan and Anarchy online had a security vulnerability which allowed a compromised server to read a clients system files and in the case of Anarchy Online, take full control of the users machine. [2]
- Online games that have social elements such as talks, chats or IM creates social engineering attacks where a users personal information or financial information can be captured for identity theft and other criminal activity. Can also be used to trick users into installing malicious software on the computer. [2]
    - Example: Most MMO’s especially ones with digital economies or where gold farming is prevalent.

[1][https://spideroak.com/privacypost/cloud-security/security-concerns-with-online-gaming/]
[2][https://www.us-cert.gov/sites/default/files/publications/gaming.pdf]