A Brief Intro to Security

December 5th, 2013

What is “Computer Security”?

“The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information systems resources”

- William Stallings, *Network Security Essentials*

The “CIA Triad”

- **Confidentiality**: A loss of confidentiality is unauthorized disclosure of data.
- **Integrity**: A loss of integrity is unauthorized modification of information.
- **Availability**: A loss of availability is the disruption of access to a system.

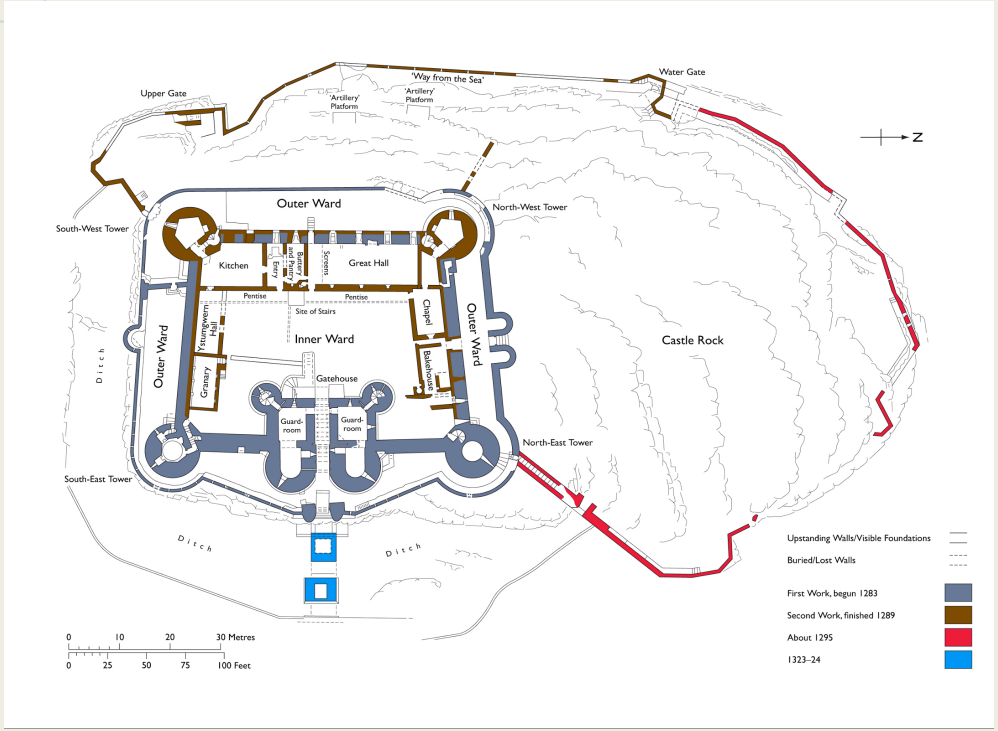
The Problem of Security

- “He who defends everything defends nothing.”
  “90% of life is solving the right problem.”
  - Mary Ann Davidson, Oracle CSO

- “Effective security is about failure.”
  - Andy Johnson, UMBC OIT

- Security is jokingly referred to as insecurity, due to the impossibility of completely protecting a system.

Defense in Depth

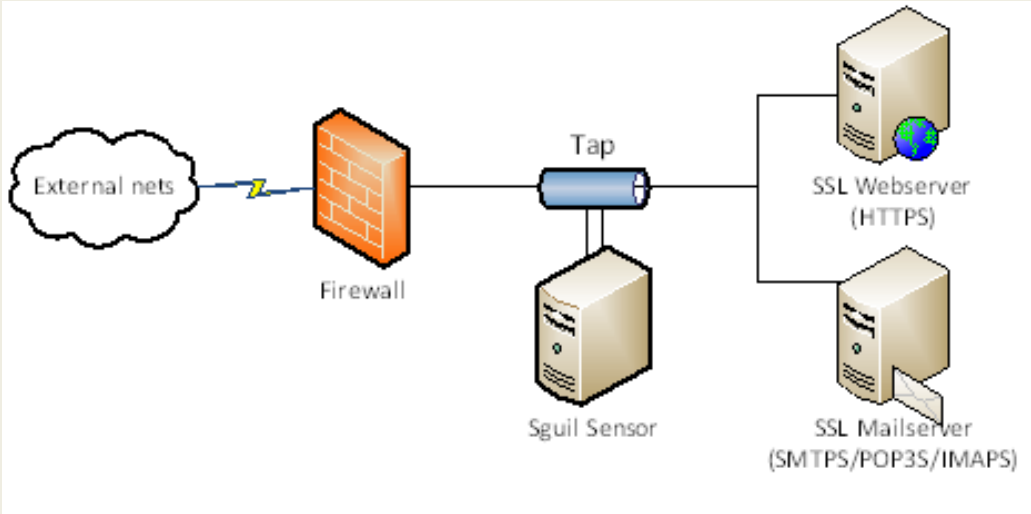


This is a model of Harlech Castle. Note the different colors of defense.

Defense in Depth expects some layers to fail, and adds enough layers to protect the keep.

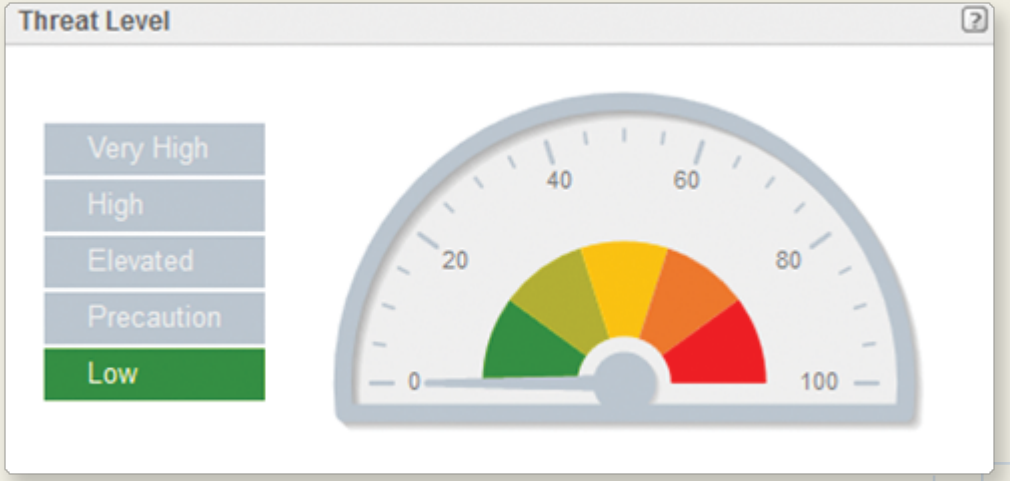
Network Defense in Depth

For a network, replace the castle layers and colors with:
- firewalls
- Internet Protocol Security (IPS)
- Secure Socket Layer (SSL)
- Verisign certificates
- various types of encryption



Continuous Monitoring

Assumes all security measures will eventually fail and constant watch to:
- ensure the most updated system
- shut down areas where attacks are getting through
- find out how they got in once areas are shut down



“Defense” Security Jobs

- Network Analyst

  In this job, the analyst is responsible for ensuring the network maintains its accessibility and integrity. This kind of analyst installs firewalls, etc.

- Security Analyst

  This job is a specific kind of systems analyst who finds and closes the security holes. Security analysts help build layers of defense by sanitizing inputs.

Dilbert's Defense

“Monitoring” Security Jobs

- Vulnerability Researcher/Penetration Tester
  Penetration Testers are given a complete system and act as attackers. They have no malicious goals other than to gain access.

- Malware Reverse Engineer
  When an attack from the “bad guys” has been detected, it needs to be prevented from spreading. These jobs usually involve deciphering attacks and creating “signatures” that can be used to identify them in the future.

CyberSecurity is a Buzzword

Hacking Matt Honan

http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/

- Hacker decides he wants Honan's Twitter Handle.
- He finds Honan's Gmail address by following link from Twitter page.
- He goes to Gmail account recovery page, pretends he has forgotten password. Gmail says "OK, we have sent a recovery password to M****n@me.com" (an AppleID).
- Hacker executes a "Who Is" search to find Honan's mailing address.
- He calls Amazon as Honan to add a credit card (verified by address and email).
- Hacker calls Amazon again, saying he has lost access. They reset account (after you verified with credit card). Now you can see last 4 digits of all account credit cards.
- Hacker now has Honan's name, address, and credit card number. He can reset the password on the M****n@me.com address, and use that to reset Twitter password. He wipes Honan's Apple account so Honan cannot trace the attack.
- Honan's reputation was severely damaged and he lost all photos from his daughter's first year of life when his Apple account was wiped.

Class Attack Activity

SQL Injection Explained:
http://www.youtube.com/watch?v=_jKylhJtPmI

1. Start your “login” by closing the username string input request. In Processing, what are strings always surrounded by?

2. The statement now has something like *username* = ‘’. This will not log you in because it will evaluate to false. How can you make it evaluate to true?

3. You don’t want to check the password - in Processing, how do you ignore the rest of a statement?

Solution: enter ‘ OR 1=1 -- into the login screen

How to Prevent SQL Injection

For those of you who are really interested (because this is a bit technical):

Use a prepared statement. This creates an escape, because it looks for the strings to be sent separately from the instruction.

```
java.sql.PreparedStatement stmt = connection.prepareStatement(
    "SELECT * FROM users WHERE USERNAME = ? AND ROOM = ?");
stmt.setString(1, username);
stmt.setInt(2, roomNumber);
stmt.executeQuery();
```

For other languages: http://en.wikipedia.org/wiki/Prepared_statement

UMBC Security Courses

CMSC 487 - Introduction to Network Security
CMSC 491 - Malware Analysis
CMSC 433 - Introduction to Web Security
CMSC 443 - Cryptology

IS 430 - Information Systems and Security
IS 432 - Computer Viruses
IS 451 - Network Design and Management

Cybersecurity graduate degree program