Chapter 1

User manual

1.1 Local installation

The game may not be permanently available over the Internet. A local installation on the PC will enable the users to access the game. Other PC or mobile phone users can also play the game without installation, as long as they are in the same local area network as the PC which serves the game. The source code of the game is downloadable at github at:

https://github.com/luyangshang/CyberCraft

To set up a server which serves the game, it's compulsory to have an Apache server first. You can choose the Apache Http Server itself, or you can choose other tools that incorporate apache server. Installing Apache Http Server itself in most cases starts from the source code, which means it tends to be more complex, with more dependencies to deal with. Therefore, this approach may bring problems for non-programmers. On the other hand, using a tool with apache inside would mean relatively a bigger installation, with modules not strictly necessary for the game also installed. However, it's a quicker solution, especially if you don't want any problems before starting running the game. The following subsections will introduce both ways.

1.1.1 Install Apache HTTP Server

The Apache HTTP Server Project itself provides only source codes, not binary. That means, you have to compile yourself to obtain the executable.

- To compilation and installation on UNIX or UNIX-like systems, refer to this page (The page is official and in detailed, so that it will not be repeated in this manual.):

  http://httpd.apache.org/docs/current/install.html

  You can use the "install" command of your OS and directly get apache2 (recommended). Alternatively, you can download the source file and compile to binary on your machine. Then you have to take care of the dependencies.

  N.B. For downloaded source file, Apache website also requires the user to verify the integrity of the downloaded files for security purpose. It provides both SHA256 hash value and PGP certificate. Except for the tools suggested on the website, one can also use the following command for a quick check of the hash values of a target file:

```
Windows 7 or later:
certiutil -hashfile <path to file>  SHA256
Linux:
sha256sum <path to file>
```

What inside the angular bracket should be replaced with the path of the file from the current directory of course. These commands calculate the hash values using SHA256 hash algorithms. Unfortunately, PGP signature is another thing, and cannot be verified in this way. Nevertheless, a matched SHA256 hash value alone is enough for the integrity check.

- To compile from source on Windows, refer to this page:

  http://httpd.apache.org/docs/current/platform/win_compiling.html

  You can build apache either from command line, or from within the Visual Studio IDE.

  After installation you can use Apache in this way:

  http://httpd.apache.org/docs/current/platform/windows.html

  It recommends running apache as a service, which runs in non-blocking mode without occupying the command line.

  Note that, if you have already installed XAMPP, you will find the contained Apache server in the folder called "apache". This contained Apache can be used the same as standalone Apache.

1.1.2 Install Tools containing Apache

There are many tools incorporate Apache like ApacheHans and XAMPP. Apache official website also recommends these tools for those who prefer executable. This part will take XAMPP as an example. After all, XAMPP features cross-platform, which satisfies users of all the current operating systems. Whereas, it should be known that other tools works also. XAMPP can be downloaded at https://www.apachefriends.org/download.html, which support Windows, Linux and OS X alike.

The default installation folder for XAMPP will be:

- Windows: C:\xampp
- Linux: /opt/lampp
- OS: X:/Applications/XAMPP/xamppfiles

This will be your root folder of XAMPP if you don't choose another path. Inside this folder, there is a subfolder called htdocs. This is where you have to copy the game (that is, the folder CyberCraft) into. For other tools apart from XAMPP, the place to copy the game may be different. Some could even put on no restriction on where the game should be. Therefore, refer to the tool's manual for the actual path.

Now, one can start the XAMPP and start the Apache server. The way varies for different operating systems, so refer to the FAQ here:

- Windows: https://www.apachefriends.org/faq_windows.html
- Linux: https://www.apachefriends.org/faq_linux.html

- OS X: https://www.apachefriends.org/faq_osx.html

When the Apache server is started, enter "localhost" (without quote) in the address bar of your browser and press enter, and you will be directed to the splash page. If by any means the server is still off, you will receive an error of connection refuse, and no page will be loaded.

Now, if you have successfully started the server, and the game is copied into the designated place, type in "localhost/CyberCraft" (without quote) and enter, you should see the game start loading. N.B. The game will try to adapt to window size before loading. Therefore, if you want to play with maximum size, you may need to load or reload the game with maximum window size.

1.2 Game beginning

When the game is loaded for the first time, you are asked to enter the name, surname and a casual 4-digit number. This name + surname + number will be your identifier throughout the game, with progress and score bound to it. When you have finished the game, and learning data collected, these triplets will be useful to identifier one player.

1.3 Tutorials

It's strongly suggested that the players start with the tutorials. In one hand, without the tutorials, the players may get stuck, even before the cyber battle really starts, not knowing what to do and how to do. On the other hand, the tutorials themselves are designed as equivalence of the later scenarios, with as much stories and gameplay as the formal scenarios. There are three tutorials.

Tutorial 1 focuses on the operations in the hall scene, which will be a preparation scene before the fight starts. The player can always quit from this tutorial through the gate, but it's recommended that he be patient enough, and finish the mission assigned by the boss.

Tutorial 2 teaches the fight in the cyberspace as defender. The defender need to use the resources to build up defense and protect the assets for a certain number of rounds. The defender has to also be careful about those attacks of DoS category, for such attacks will consume the server capacity, which makes you earn less resource in the next round. The defender should fix as much holes as possible before the intruder starts attacking in the next round. It should also be noted that, many fixes expire with time. If a fix has expired, and the defender has forgotten to re-apply it, the assets or the server being protected, will be again exposed to the related attack.

Tutorial 3 is about the fight in the cyberspace as intruder. The intruder earns a small amount of resource as the turn goes, but a better way to gain resource is by dealing damage to the assets under the protection of the defender. However, the intruder should choose the attack pattern carefully, as some of the vulnerabilities might be temporarily or permanently fixed by the defender. There are four types of offensive acts:

- The acts as "Finishing move", which directly deal damage to the assets. They are clearly the most liked type of attack. They deal significant damage to the assets, while also granting bounty for the damage dealt. Nevertheless, in the majority of cases, the intruder can only successfully perform these attacks once each round. Moreover,

attacks of the second category are usually needed to break the defenses, before attacks of this category to succeed.

- The acts without “Finishing move”, ”Dos category” or “Improvement”, has little or no damage. These attack are used to create or remove buffs on the rival (marked with “Rival +” and “Rival -” respectively), which open door for subsequent attacks, e.g. one of “Finishing move” category.
- Attacks marked with “DoS category” targets the server or the service, instead of the assets. These attacks force pressure on the server (displayed as the buff “Denial of service attacked”), which hamper the server from serving client requests in the next round, decreasing the defender’s resource income.
- Attacks marked with ”Improvement” are self-improvements to increase the effectiveness of other attacks. Some improvements are presented with buffs. Then the corresponding acts are marked with “Self +”.

There is no strict limitation on how many acts can be applied in each round as long as the resource is adequate. Nevertheless, players should end their turn when there is nothing that they can do in the current round.

What defenders can do before ending the round: fix more vulnerability with defensive acts, whether protecting the assets or protecting the server. Reapply defensive technique before the corresponding buff expires will refresh the buff length (if the new length is longer).

What intruders may do before ending the round: 1. Organize a “Finishing move”, potentially preceded by some acts of category 2. 2. Perform an attack of DoS category 3. Perform “Improvement”. Point 1 is the always the primary goal for each round. The intruders would in general catch every chance for that. Point 2 and point 3 are optional, intruder may decide whether it’s worthy, based on the sufficiency of his/her resource. Sometimes, if the intruder sees all the possible paths for the attacks are blocked, he/she could even directly end the turn.

1.4 Scenarios

With “Play” button you can enter the scenario selection scene (1.1). The scenarios are made in pairs, and will also be unlocked in pairs. In each pair, the first scenario is the one with even scenario number, where you play as an intruder(who is called Christopher); the second scenario is the one with odd scenario number, where you play as defender(who is named Godfried). As can be seen in the figure, “highest Score” will be noted down for each scenario completed. Successful completion of both scenarios of the previous pair will unlock the next pair. The player can repeat scenarios already completed, to get higher score or to perform better. The AI has its a preset action patterns for the specific scenario, but it will act differently each turn. Therefore, repeating the same scenario usually resulting in different situations where the player has to adapt himself/herself to it.

1.5 Hall

The company’s or HackIt’s hall is the place where the player receive his/her mission before he/she enters cyberspace to fight his/her rival. Besides mission briefing from the boss, players can also wander around, talking to other NPCs in the hall. These NPCs will provide the players with more

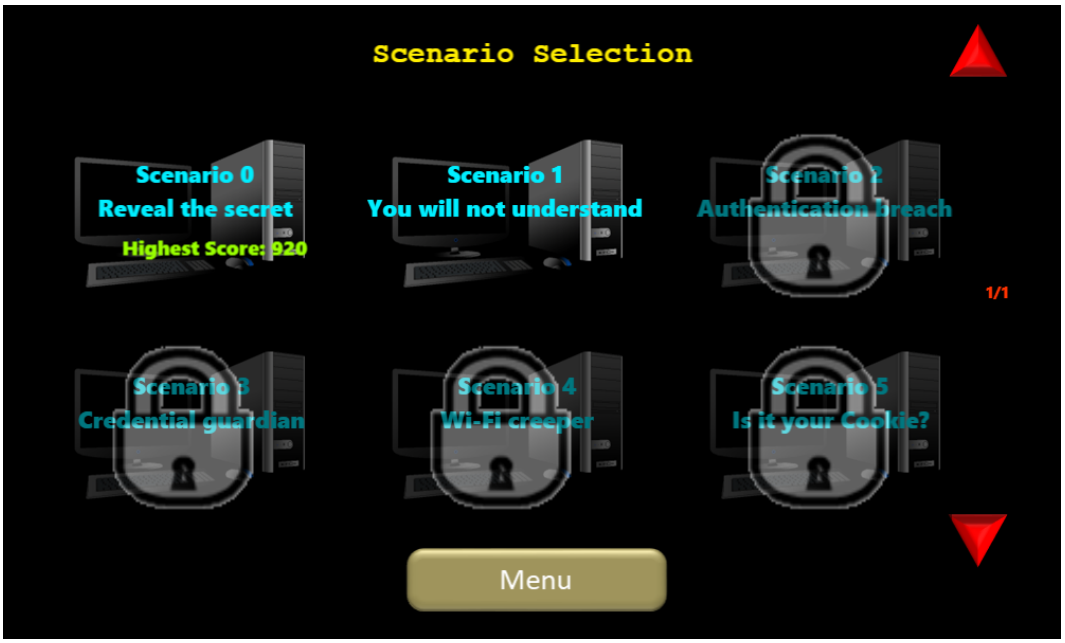

Figure 1.1. Scenario Selection

information about the upcoming fight, and will occasionally give some hints and suggestions to the players. Therefore, when starting a new pair of scenarios, it's a good practice to talk to the NPCs, so as not to be totally confused when seeing the new acts.

1.6 Acts and buffs

The acts represent a security action that the character do to achieve the goal. The intruder uses cyber security attacks, denoted as offensive acts. These acts usually deals damage to the assets or impair the opponent, opening door for future attacks. The defender uses defensive techniques of cyber security, sometimes called as defensive acts, to enhance the defense of all kind, so that the service being protected will survive longer.

However, not all acts take effect immediately. Some acts could even have some lasting effects, which will remain for a certain number of rounds, or even forever. All this lasting effects are called buffs. The buffs represent that something is in use, or the state that an attack in progress. For example, a "MITM" attack performed by the intruder will, on success, give the defender a "MITM" buff. This buff, before expiration, will allow the attacker to perform a "Sniffing attack", which will deal considerable damage to the assets, which is under the protection of the defender. On the other hand, the defender can apply the defensive act called "MQV" (an authentication protocol) to obtain the buff of that name, which nullify future "MITM" attack, until the buff expires.

N.B. besides the acts enforcing buffs, there are also the acts that cleaning buffs on the character. This happens when the intruder breaks some kind of defense, or when the defender turns to alternative technique in place of the old one. Figure 1.2 gives the explanation of all the possible relation between the acts and the buffs.

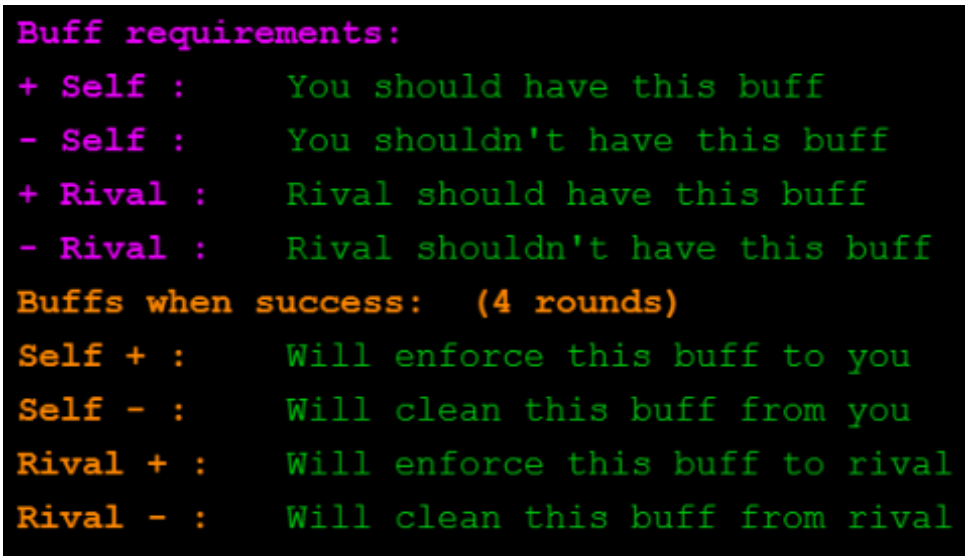

Figure 1.2. Requirements on buffs and effects to the buffs that might be found on an act

1.7 Cyberspace

The fight in the cyberspace always starts with the defender's round. However, the defender need to calculate his/her resource carefully, as he/she usually does not have enough resource to strengthen on all aspects. The intruder, on the other hand, exploits these defenseless points. The main screen of cyberspace is given as figure fig:cyberspaceWithDescription.

Personal notes

If the player is a new comer, and is unfamiliar to the terms referred to in the game, he/she may need to frequently refer to personal notes. It can be opened with the book-like button on the top-left corner of the screen, or using a shortcut key N. But a better way is to use the button near the act description or buff description (shortcut key is also N). The buttons at act description or buff description will go directly to the specific entry in personal notes, which saves the player's effort to search for the term. There are also internal links where the player can navigate to other correlated terms. A chain-like button will also lead the player to external resources, to facilitate those who are interested to know more.

Except for the personal notes used for the explanation of the terms, other two things are frequently referred to. They are buffs on the character and action log.

Buffs on the character

By clicking on the portrait of the player avatar (or with a "S" key), one will be able to see the buffs on the avatar. Similarly, by clicking on the rival's portrait (or with a "R" key), the player will be able to see the buffs on the rival. Nevertheless, most of the buffs are supposed to be found on the defender. The intruder will (frequently) check the buffs on the defender, especially those positive buffs, which represent the defense that has been set up. The intruder should strike only the defenseless point or at least those that are not very well defended. On the other side, the defender will check the buffs on him/her, to know where needs more strengthening.

Action log

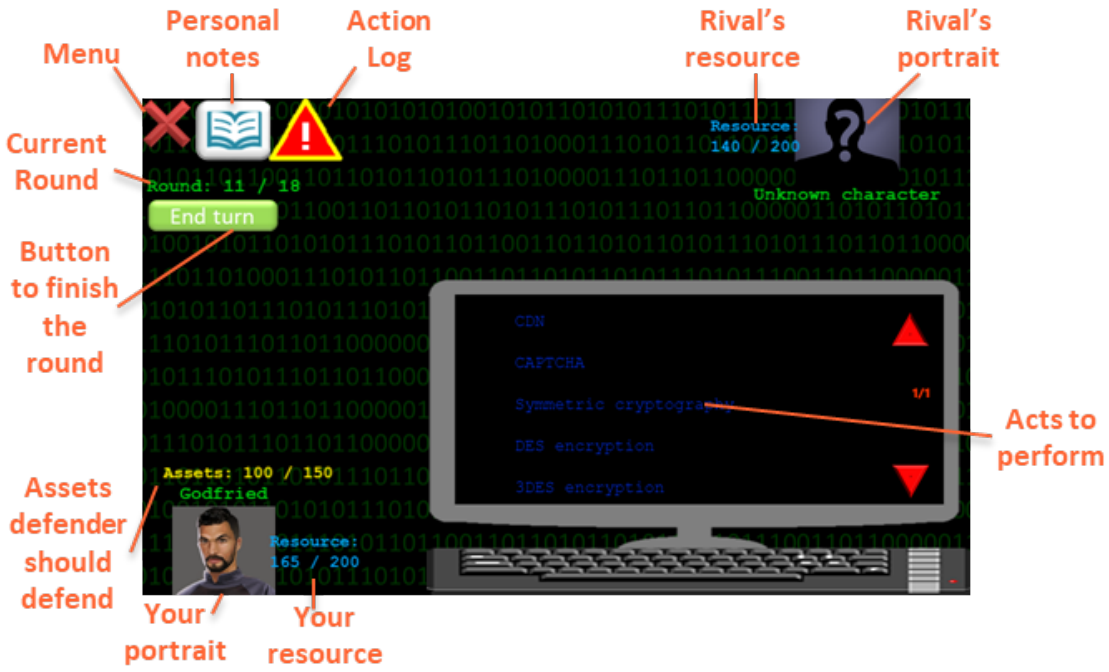

Figure 1.3. The main scene of cyberspace

The other place to refer to is action log. It can be opened by clicking on the exclamatory-mark-sign on the top-left corner of the screen, just adjacent to personal notes. The action log is actually a log of the history. It notes down the acts performed by the characters, as well as whether they succeeded. This allows the player to refer to past rival acts when he/she just missed it. However, the most important value of this action log is when an act fails. The reason of why the act failed will be of great value to the player, especially the new comer who cannot remember things well. The reasons of the failure contain the presence or absence of necessary buffs, as well as the lack of luck: not all acts can be performed with 100% success rate. By clicking on one entry, the player can see the reason why the act failed. And, by clicking on the name of the act (called as Act pattern) specifically, the player can read its explanation in the personal notes.

1.8 Review

The review scene displays more or less the same as action log that the player is able to read in the cyberspace. Whereas, the review scene gives the player one more chance to revise how he/she has done during the scenario. If the scenario failed, review is an excellent place to know what is wrong, and brace oneself and prepare for one more trial.

1.9 Formulas

Advanced players and hardcore gamers are always interested in calculation formulas in the game, so that they can plan their strategy more quantitively.

1.9.1 Formula for the score

When the cyber battle ends, the outro scene will be shown, where the player's score will be calculated, mainly based on the performance noted in action log. The calculation formula is listed in figure 1.4. The formulas tell that the intruder should strike fast and strike fierce. The defender, however, should concentrate on building an invincible defense, no others.

Events	Change to intruder's score
Each successful act at his round	+90
Each round defender survives (including round 1)	-50
Each damage to the assets	+5

Events	Change to defender's score
Each failed act at intruder's round	+100
Each round he survives (including round 1)	+50
Each damage to the assets	-5

Figure 1.4. score calculation formulas for the intruder and the defender

1.9.2 Formula for served requests

The defender obtains resource only at the start of his turn, based on the number of client requests served and unserved. Each served (happy) client grant 10 resources, while each unserved (unhappy) client subtracting 5 resources. The following formula will be a little complex, and is intended for hardcore gamers only.

The number of served clients is calculated based on the server capacity, the number of client requests, the number of spam requests brought by the intruder, and the defender's DoS resistance. Legitimate client requests could vary each round, but only within the minimum and maximum threshold specified in the scenario's cyber file. Let's suppose the number of legitimate requests of this round is L, and the server's current capacity is C, the served requests is S, unserved requests is U. Then:

If L <= C , S = L, U = L - S = 0

If L >C, S = C, U = L - S = L - C

At the presence of intruder's spam requests, things become peculiar. Let the intruder's (total) spam request be F, defender's (total) DoS resistance be R (R = 1 - (1- R1) * (1 - R2) * (1 - R3)...). Then the effective spam request EF = F * (1 - R).

If L + EF <= C, still S = L, U = 0 — the server is powerful enough to sustain, even when attacked;

If L + EF >C, then C / (L+ EF) = serving ratio = S / L

(Effective spam request are treated the same as legitimate requests)

That is to say, S = Floor(C * L / (L+ EF))

(Round to integer is necessary. After all, there should not be "a half" client served)

There are many things that hardcore gamers can be deduced from this formula. But the most important one are:

- Increasing the capacity improves the served clients linearly when the server is destined to decline some clients.
- Continuously increasing the spam request increases the effective spam requests linearly. However, as the number of spam requests increase, boosting the spam requests results in less and less additional unserved requests. Therefore, the intruder should never try to block all legitimate requests. It just does not worth the effort.

1.10 Extra guide for the scenarios

This part is not intended for players who have not played the game.

The players are supposed to discover how to maneuver against the rival exactly. Information from NPCs, act/buff details, personal notes, action logs, previous trial of the game, or even external materials all contribute to it. Nevertheless, if the player has already retried a scenario several times, but still cannot sort out the potential paths for the intrusion or for the defense, here are some illustrations for the attack paths of the scenarios.

In the figures, red explosion indicates the offensive acts, while blue shield indicates defensive acts. Arrows starting from nowhere shows this is a possible starting point for the intruder. Shield before an explosion means that such defense can defeat the following attack, and eventually, block the attack chain. However, there are also bypasses where the intruder can still prevail despite the defense, which is illustrated as branching.

It's can be easily found that, at each round when the intruder plans attack, he should never choose a chain on which some defense is built, except there is also a bypass. On the other hand, the defender always tries to fortify on every path, and try to maintain this state for as long as possible. N.B. only clear blockings are listed in the figures. There are also other acts which increase or decrease success rate, which are not shown in the figures.

Scenario 0, 1:

The two scenarios share the same pattern. The player only plays in different roles.

From figure 1.5, one can see that, there are 5 possible attack chains. As a matter of fact, the first three ends with "Sniffing attack", and deals a significant damage. "DH" is one kind of defense on these attack chains, but MITM can be used to bypass it. "MQV" and "RSA key exchange" avoid "MITM", but Quantum computing defeat them all. Then "Quantum criptography" becomes an ultimate defense on these attacks. The fourth chain, "replay attack" goes another way and deals normal damage. This path is thus taken as a second choice when the former attacks are impossible. The fifth path actually deals no damage, but it creates an effect of DoS on the rival. This effect should not be overlooked through, for the defender gets scarce resource, and may not be able to put up a fight.

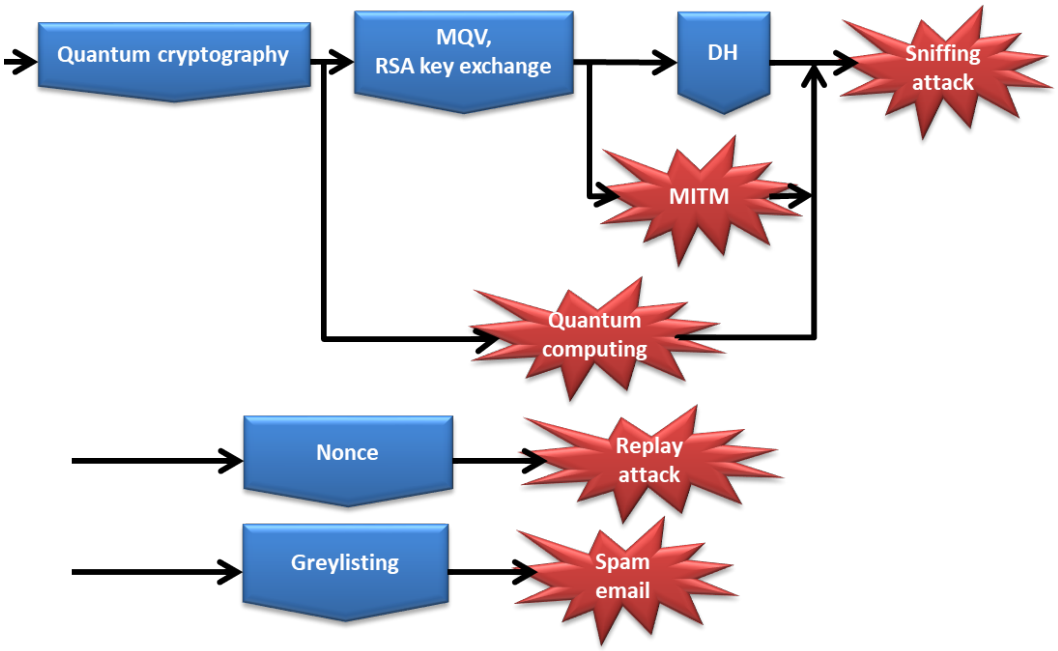

Figure 1.5. Intrusion patterns and their defenses for scenario 0 and scenario 1

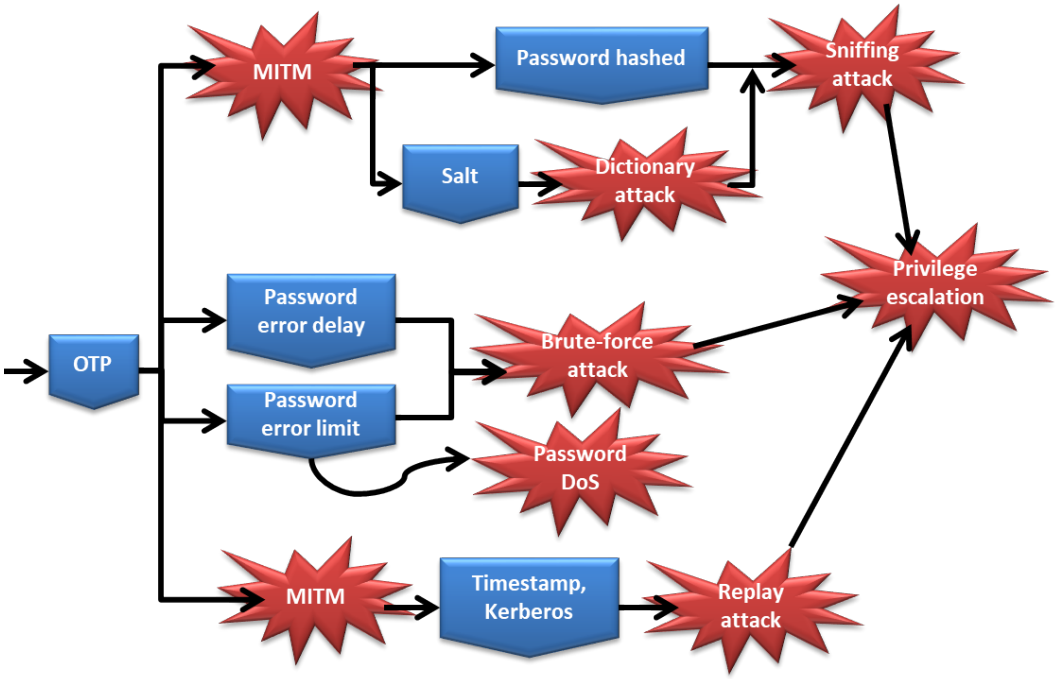

Figure 1.6. Intrusion patterns and their defenses for scenario 2 and scenario 3

Scenario 2, 3:

The two scenarios share the same pattern. The player only plays in different roles.

Figure 1.6 illustrates that, "dictionary attack" provides a bypass through "password hashed", but it still has its nature enemy. "Password error limit" fights "Brute-force attack, but it adversely opened door for "Password DoS" attack.

It's interesting to see that, "OTP" is a panacea to keep away from any attacks in these scenarios. Senior gamers would immediately guess that "OTP" will be greatly costly. You guess it right. It's usually used in the last rounds to guarantee you rest easy.

An unique offensive act unlocked during these scenarios called "Privilege escalation" greatly enhances the strength of the intruder. It's used only after a successful credential compromise, dealing an extra great damage to the assets.

One think not illustrated in the figure is that, you gain additional resource in this scenario by providing the functionality of single sign-on. It can be provided by a "Password manager" or "Kerberos".

Scenario 4, 5:

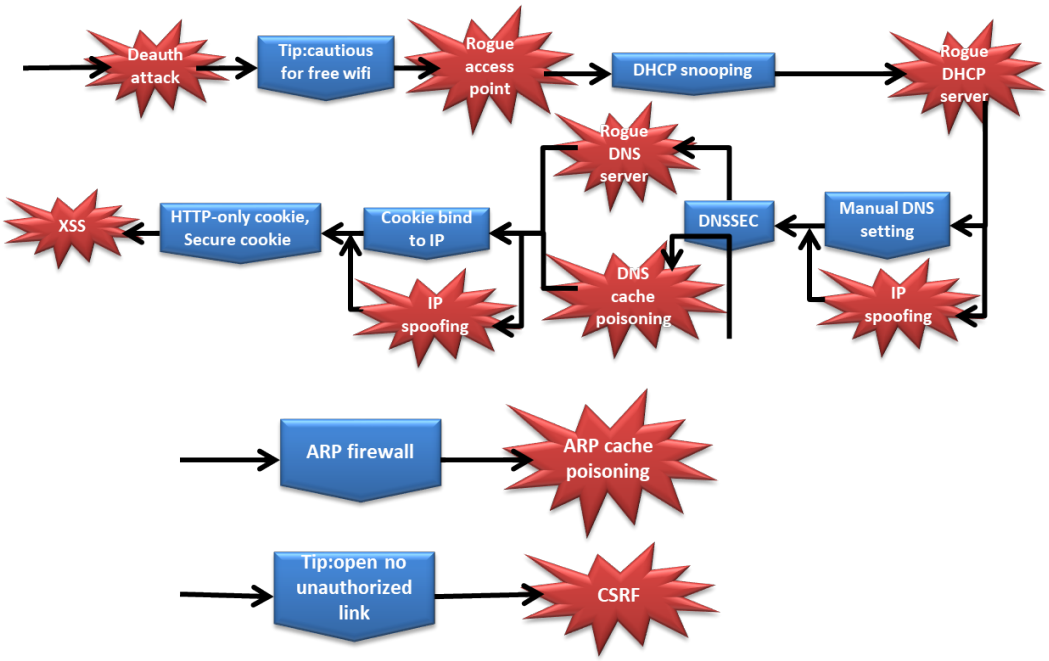

Figure 1.7. Intrusion patterns and their defenses for scenario 4 and scenario 5

The two scenarios share the same pattern. The player only plays in different roles.

It's demonstrated in figure 1.7 that, some attack chains have prolonged length. But don't worry, the intruder also gets partial success on the "milestones" in the attack chain (e.g. "DHCP hijacked", "DNS hijacked"). Nevertheless, for quick and fierce attack, successful "XSS" attack and "CSRF" attack are the really targets. "IP spoofing" is found here as bypass through two defensive acts, which are intrinsically IP-based techniques. "ARP cache poisoning" has its own attack chain here, but it does not come with great damage or great bounty for the intruder, so

don't overestimate it. There are four potential attack chains in this pair of scenarios. The first one starts with "Deauth attack", but the second one starts half way, at "DNS cache poisoning".

A unique act for this pair of scenarios is "(Wi-Fi) Deauth attack". It's not defendable, and it kicks the defender offline. This means the defender can do nothing in the next round. If some defensive approach expires in that round, he cannot renew it. Therefore, the defender may have to renew buffs before the expiration date, if he suspects the intruder is preparing this attack. From the intruder's perspective, "Deauth attack" is obviously a good supporting technique for overwhelming assault.