Reply attack

به طور کلی دو نوع پیام در سرور مخابره می شوند پیام هایی که محرمانه نیستند مث ویژگی محصولات و پیام های محرمانه ویژگی کاربران و ... برای نوع اول نیاز به رمز خاصی برای دیدن پیام ها نیست و صرفا پیامی به صورت زیر باشد درست می باشد که مقادیر توکن و یوزرنیم برای این پیام ها مقادیری ثابت اند:

```
String result = "this is a client" + "--1989--" + MenuHandler.getToken() + "--1989--" +
        command + "--1989--" + System.currentTimeMillis() + "--1989--" +
        ((MenuHandler.getUsername() == null) ? "no username" : MenuHandler.getUsername());
return result;
```

توجه کنید که کل عبارت کد دار است و بدون دسترسی به کد های کلاینت غیر ممکن است که به اطلاعات دسترسی داشت پس دو اتفاق ممکن است، عین خود پیام فرستاده شود یا به کمی تغییر، در سرور اگر ip ای سعی کند بیش از 10 پیام در ثانیه بفرست به لیست سیاه منتقل شده و دیگر اجازه وصل شدن ندارد و اگر هم پیام با فرمت اشتباه پس از decode شدن دریافت کند بازم هم همین طور اجازه وصل شدن از آن ip سلب میشود.

قطعه کد زیر نشان می دهد که اگر پیام ارسال شده پس از 100 میلی ثانیه ارسال شود هم نامعتبر است که یعنی اگر پیام ها شنود و ذخیره و سپس بعدا ارسال شود بازم هم نامعتبر می شود و ip بلاک می شود.

```java
String token, message, username;
long time_sent;

try {
    token = command.split( regex: "--1989--")[1];
    message = command.split( regex: "--1989--")[2];
    time_sent = Long.parseLong(command.split( regex: "--1989--")[3]);
    username = command.split( regex: "--1989--")[4];
} catch (Exception e) {
    System.out.println("we're under attackkkkkkk");
    blackListOfIPs.add(getIP(socket));
    return;
}

//the time is old

if (System.currentTimeMillis() - time_sent > 100) {
    blackListOfIPs.add(getIP(socket));
    return;
}
```

پس در صورت داشتن الگوریتم کد شدن پیام ها در کلاینت، می توان به اطلاعات غیر محرمانه دسترسی داشت ولی نمی توان به صورت گسترده پیام فرستاد چون ip مذکور بلاک می شود همان طور که قطعه کد زیر نشان می دهد.

```
//making sure it doesn't send more than 10 requests in 100 milliseconds

if (IP.addIp(getIP(socket))) {
    blackListOfIPs.add(getIP(socket));
    return;
}
```

```
public static boolean addIp(String Ip) {
    IP ip = getIp(Ip);
    if (ip == null) {
        new IP(Ip);
        return false;
    }
    if (ip.ip.equals(Ip)) {
        if (ip.tenRecentTimes.size() >= BOUND) {
            ip.tenRecentTimes.remove( index: 0);
            ip.tenRecentTimes.add(System.currentTimeMillis());
            return ip.tenRecentTimes.get(BOUND-1) - ip.tenRecentTimes.get(0) < 100;
        } else {
            ip.tenRecentTimes.add(System.currentTimeMillis());
        }
    }
    return false;
}
```

برای اطلاعات محرمانه هم، در صورت نداشتن الگوریتم های کلاینت کاملا مشابه حالت بالا است که یا پیام زیاد می فرستند و اصلا به لیست سیاه منتقل میشود یا پیام را اگر دیر بفرست بازهم چون پیام ها زمان دار هستند پیام بررسی نمی شود و ip بلاک می شود و اگر هم پیام تغییر داده شود به احتمال بالا، فرمت ان پس از دیکد شدن اشتباه می شود و مشابه بالا می شود.

پس فرض کنید که به الگوریتم های کلاینت دسترسی داریم. اما چون که الگوریتم رمز سازی توکن که شامل اطلاعات مهمی همانند یوزرنیم و زمان ساخت توکن است را نداریم و صرفا منوط به آگاهی کامل نسبت به سرور است پس آنها دست نخورده می مانند و توکن یک کاربر برای کاربر دیگر اگر فرستاده شود، سرور آن ip را بلاک می کند چون که username توکن را با username پیام تطبیق می دهد.

```
if (Token.isTokenValid(token)) {

    try {
        String decodedToken = Token.decode(token);
        long time = Long.parseLong(decodedToken.split( regex: "--caption neuer--")[0]);
        Account account = Storage.getAccountWithUsername(decodedToken.split( regex: "--caption neuer--")[1]);
        if (!Token.getUsernameFromToken(token).equals(account.getUsername())) {
            throw new Exception("piss off");
        }
    } catch (Exception e) {
        System.out.println("we're under attack by trying wring tokens");
        blackListOfIPs.add(getIP(socket));
        return;
    }

    //checking that it's still authentic

    if (!Token.hasTokenExpired(token)) {
        Server.server.takeAction(message);
        Token.addOnlineUsers(Token.getUsernameFromToken(token), System.currentTimeMillis());
    } else {
        Server.server.takeAction( command: "token has expired");
        Token.addOnlineUsers(Token.getUsernameFromToken(token), (long) -1);
    }
}
```

پس پیام می تواند صرفا برای همان username مربوط به توکن باشد، در این حالت اگر پیام های زیاد فرستاده شود که قبلا وارسی شده است، و اگر اطلاعات دیگری در قسمت message خواسته شود صرفا همان کار هایی است که با خود کلاینت هم میشود به آن دسترسی داشت (!!!) که غیر منطقی است کسی وقتی با خود اپ می تواند این کار را انجام دهد با کد دیگری انجام دهد و این حالت در حقیقت در broken authentication بررسی شده است .

و اخرین راه کار که بسیار هم کارامد است این است که هر account یک ip دارد که موقع لاگین دریافت می گردد و اگر کسی سعی کند به اطلاعات ان کاربر با ای پی دیگر دسترسی داشته باشد بلاک می شود:

```
// making sure it's got one ip

Account account = Storage.getAccountWithUsername(username);
assert account != null;
if (account.getIp() == null) {
    account.setIp(getIP(socket));
} else {
    if (!account.getIp().equals(getIP(socket))) {
        System.out.println("we're under attack by wrong ip");
        blackListOfIPs.add(getIP(socket));
        return;
    }
}
```