Survey on Web Servers Vulnerable to Drown Attack

Avinash Ravi (avinravi@indiana.edu)
Sravya Gudipudi (sgudipud@indiana.edu)

Motivation and Background:

DROWN (**D**ecrypting **R**SA with **O**bsolete and **W**eakened e**N**cryption) is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS. It is a new form of cross platform Bleichenbacher padding oracle attack that allows an attacker to decrypt the intercepted TLS sessions and gain access to passwords, credit cards and other sensitive information. Modern servers use TLS protocol for secure communication with the client. There are other versions of SSL like SSLv2, SSLv3 of which SSLv2 is vulnerable to many attacks. But the servers are configured to accept SSLv2 connections to support legacy clients. DROWN attack shows that merely supporting SSLv2 in the servers is a threat to TLS connections. A server is vulnerable to DROWN

- If it allows SSLv2 connections, or
- If it's private key is shared with other servers that allows SSLv2 connections. This is common configuration in servers to use the same certificate for multiple servers like email, web servers.

Background on DROWN Attack:

SSLv2 Handshake – In SSLv2, a client initiates a connection by sending a ClientHello message to the server which includes a list of cipher suites supported by client and a client nonce. The server responds with a ServerHello which includes the list of cipher suites supported by the server, server nonce and public key of the server. The client then responds with a ClientMasterKey message that includes the cipher suite selected and a master key. For export ciphers, 11 bytes of this master key is sent as plain text and 5 bytes is encrypted. For non-export ciphers, the master key is completely encrypted. The server responds with a ServerVerify message and client responds with a Client-Finished message. Sever completes the handshake with a Server-Finished message. One of the vulnerabilities in SSLv2 is that the part of master key is sent as a plain text for export ciphers and can be decrypted by brute force.

PKCS#1 v1.5 Encryption Padding – SSL/TLS uses PKCS#1 v1.5 which pads the messages with random bytes of string before encryption. A random padding string PS is generated and appended to the message as 00||02||PS||00||message. The server that decrypts this message returns an error if the decrypted message is not PKCS#1 v 1.5 complaint. This leaks some information and Bleichenbacher attack makes used of this vulnerability to decrypt the key in SSLv2.

DROWN Attack:

The attack flow of DROWN attack to compromise a TLS session using SSLv2 is:

- The attacker collects many TLS handshake key exchange messages. If the attacker's main target is a server, then the server can be observed for TLS connections from many clients. If the attacker's victim is a client, the attacker has to patiently wait to collect as many TLS connections.
- The attacker then converts the collected TLS key exchange messages into SSLv2 conformant PKCS#1 version 1.5 messages using a technique described by Bardou et al which involves complex mathematical operations.
- After obtaining the SSLv2 conformant messages, Bleichenbacher attack can be performed on the SSLv2 conformant messages to decrypt the TLS handshake key messages. Bleichenbacher attack makes use of the fact that only a part of the premaster secret is encrypted in SSLv2 rather than the whole premaster secret for export ciphers. There is

modified version of Bleichenbacher attack that exploits the TLS handshake mechanism where server sends a ServerVerify message before the client has authenticated itself. These two methods are used to guess the premaster secret using brute force.

- Once a premaster secret is obtained, the client write key and server write keys are computed which can be used to decrypt the whole TLS session.

Defense against a DROWN Attack:

Nothing can be done from the client side to prevent DROWN attack. The servers need to be updated to use a different certificate for servers that support SSLv2. Also, OpenSSL and Microsoft have released patches for countermeasures against DROWN attack and the servers need to be updated to include these patches.

Points to be noted:

- DROWN attack does not reveal the private key of the server, but instead compromises the communication messages of a single session.
- The DROWN attack requires a lot of computing power and will take 2^{40} symmetric encryption operations for a 40-bit export cipher.
- Bleichenbacher oracle padding attack cannot be performed on TLS since there are countermeasures in place for this attack implemented in SSLv3 and higher versions, but there are no counter measures for this attack in SSLv2.

Our proposal and its Contributions:

We are proposing to do a survey on top 1 million websites for identifying the websites or its included servers that are vulnerable to DROWN Attack. Survey focuses on evaluating how many websites are still supporting SSLv2 along with TLS and also how many of them support weak encryptions (export ciphers) for SSL handshake. We also identify the highest SSL/TLS versions currently supported by the web servers. Our goal is to finally categorize the results based on top level domains to identify what kind of top level domain (for example .edu or .com) websites are mostly supporting SSLv2 and combined with weak encryptions.

We believe that our project survey can be used to learn how many Web servers are still not been patched against DROWN attack. Before DROWN, even if SSLv2 is enabled along with TLS, as most client are updated to use TLS, it is not found to cause any security hole. But with DROWN attack we can break TLS session by exploiting vulnerabilities in SSLv2, so it is very important that the vulnerable servers are patched as soon as possible. The Patch for DROWN is released by OpenSSL very recently, so there is high chance that there will be many servers that are vulnerable.

Important point to note here, although we are evaluating a huge number of websites, there we will be servers, which are hiding under the firewall that are vulnerable to DROWN. Such web servers can only be tested from server side and hence, cannot be included in our study.

Preliminary Techniques:

Basic tentative Skelton of the model we are developing for the project:

- We will develop a scanner for the DROWN vulnerable websites. The scanner will be run across top 1 million websites listed by Alexa.
- We expect the scanner to pick each website from the listing and identify HTTPS connection by this website. We are currently looking for proxies to intercept HTTPS connections from the website.
- It will also force initiate SSLv2 connections on Servers that are supporting SSLv3 /TLS to check if the server still supports SSLv2.
- And it will look for weak encryptions supported by SSLv2 servers as it will enable DROWN attack.

Evaluation plan and Timeline:

Following a brief tentative plan for the project we are proposing. The plan might change and evolve to adapt to final project development.

1) Week 1 [March 22 – March 27]: We will do the back ground work needed to start the project, concentrating on resources that we can utilize when building the project. Our study includes but not limited to
   - Reading the DROWN paper again for better understanding of the attack and reading any other related articles that can help us.
   - Identifying the best application that we can use to intercept HTTPS connections and
   - Reading and understanding OpenSSL documentation to identify and understand execution of commands, which we can use to evaluate on the highest version of SSL/TLS, SSLv2 support and supported encryptions.
2) Week 2 [March 28 – March 7]:
   - Working on development of a model to scan top 1 million websites ranked by Alexa.
   - We expect this scan to identify and report on SSLv2 support, highest version of SSL/TLS supported and about any week encryptions used as described in DROWN Paper [1].
3) Week 3[April 8 –April 13]:
   - Testing the model that we develop in week 2 in incremental fashion until we are confident enough to run an entire scan on all websites.
   - Run the scan, which we expect to for days (all websites).
4) Week 4 [April 14 – April 19]:
   - Continuing the scan, if any websites are remaining from week 3.
   - Consolidating the results and writing an evaluation report. Report process will be taking longer as we intend to categorize the report by top level domains.

References:

1. *DROWN: Breaking TLS using SSLv2* by Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar and Yuval Shavitt.
2. https://drownattack.com/