Team: Password Is Password

Mohit Jangid, Eric Lewantowicz, Joseph Shaffer

CSE 5473

4/22/2018

**Bleichenbacher and POODLE SSLv3 Padding Attacks**

**POODLE Attack**

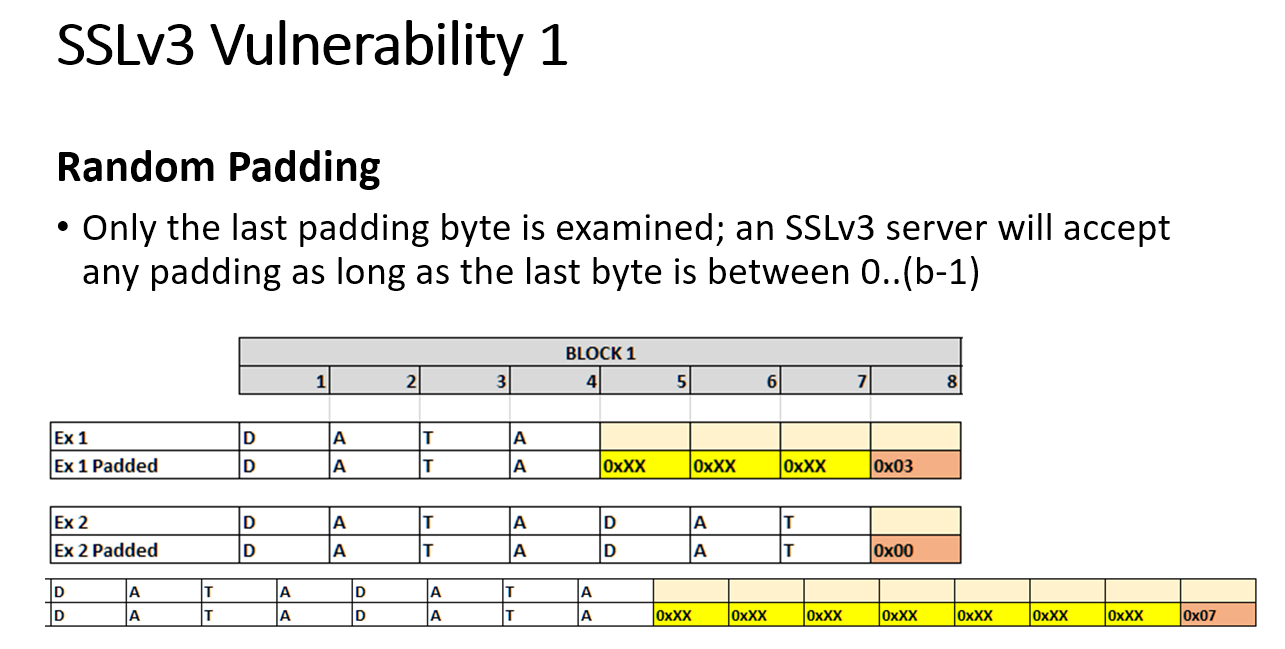
**Goals**

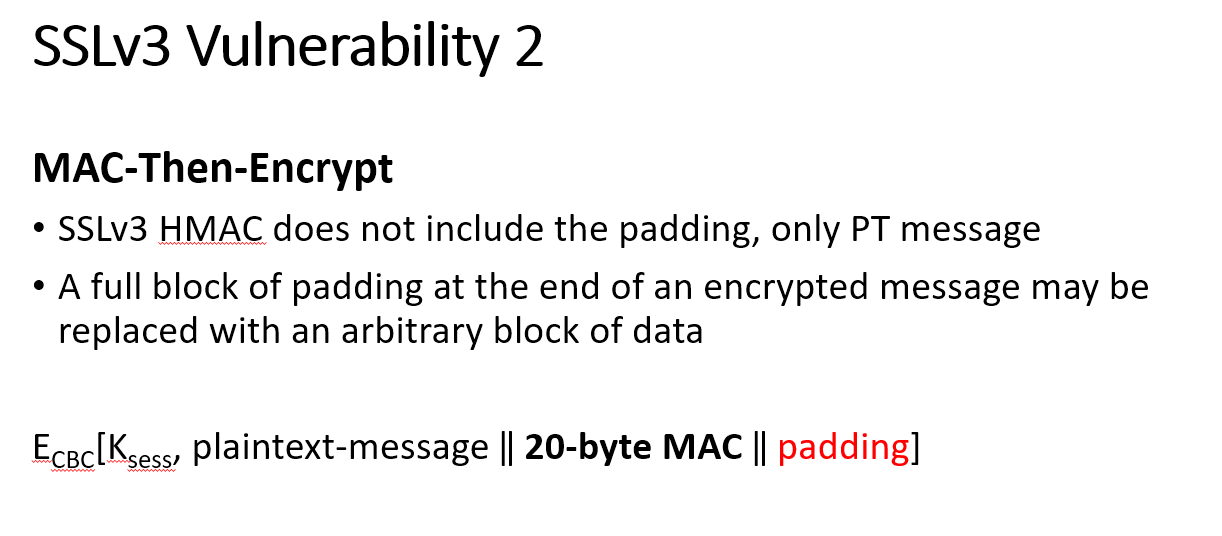
1. Learn the vulnerabilities of SSLv3 encryption scheme and the details of the POODLE attack.
2. Implement the SSLv3 protocol at a low-level from scratch in Python 2.7 with the Pycrypto module, with combined Client/Attacker communicating with Server Oracle over TCP stream sockets.
3. Write a GUI from scratch using Curses shell graphics module in order to provide an effective visualization of the attack simulation.
4. Consider possible defensive approaches and implement a defense against a POODLE attack.

The Padding Oracle On Downgraded Legacy Encryption attack was discovered by a Google Security team in 2014. It is a man-in-the-middle attack on the (at the time) deprecated but still supported SSLv3 encryption scheme using block CBC mode. Because many servers still supported SSLv3 in order to support legacy applications and browsers still employing it, an attacker could execute a “downgrade dance” to cause a browser and server to fallback to an SSLv3 encryption scheme. Using elements from the BEAST attack (see references), an attacker can inject an HTTPS request generator into a victim client’s browser using JavaScript injection from a complicit HTTP website. The attacker could then use the request generator to fashion plaintext messages, that combined with a secret cookie, would be encrypted with SSLv3 and then sent to an HTTPS server. The attacker intercepts the encrypted traffic, moves the ciphertext block containing the secret cookie to the end of the message, replacing a full block of padding, and then forwards the modified encrypted message to the server. The server acts as an oracle and disconnects the session if the padding or MAC is incorrect, and accepts the message if the padding is correct. This process allows the attacker to decrypt the contents of the message, i.e. the cookie, byte by byte.

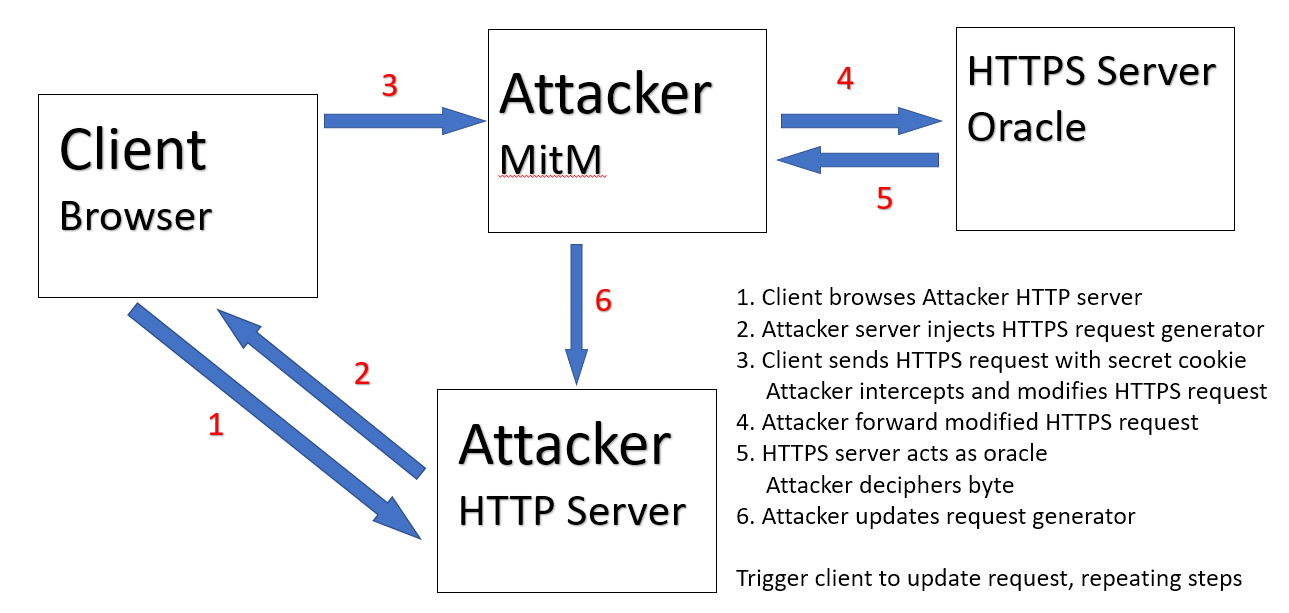
After discovery of the POODLE attack, the long-term solution was to eliminate SSLv3 support altogether in all browsers and servers, since the RC4 stream variation of SSLv3 has its own vulnerabilities and is not considered secure. However, several short-term mitigations were proposed and implemented in the short term, including anti-POODLE record splitting by the Opera browser. While we didn’t find any details on their record-splitting approach, the idea served as the seed for our own record splitting defense proposal.

**Key SSLv3 vulnerabilities that the POODLE attack exploits** (graphics from our PowerPoint presentation)





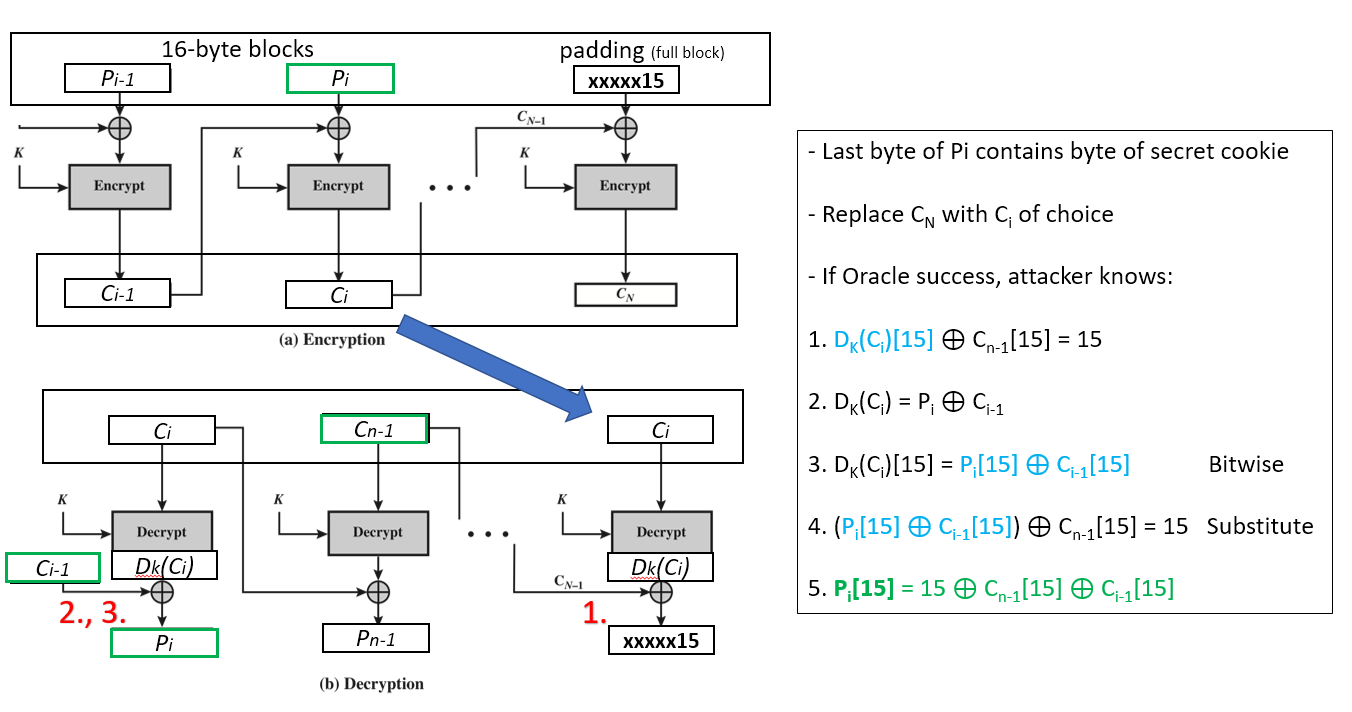
**Attack overview** (diagram from our PowerPoint presentation)



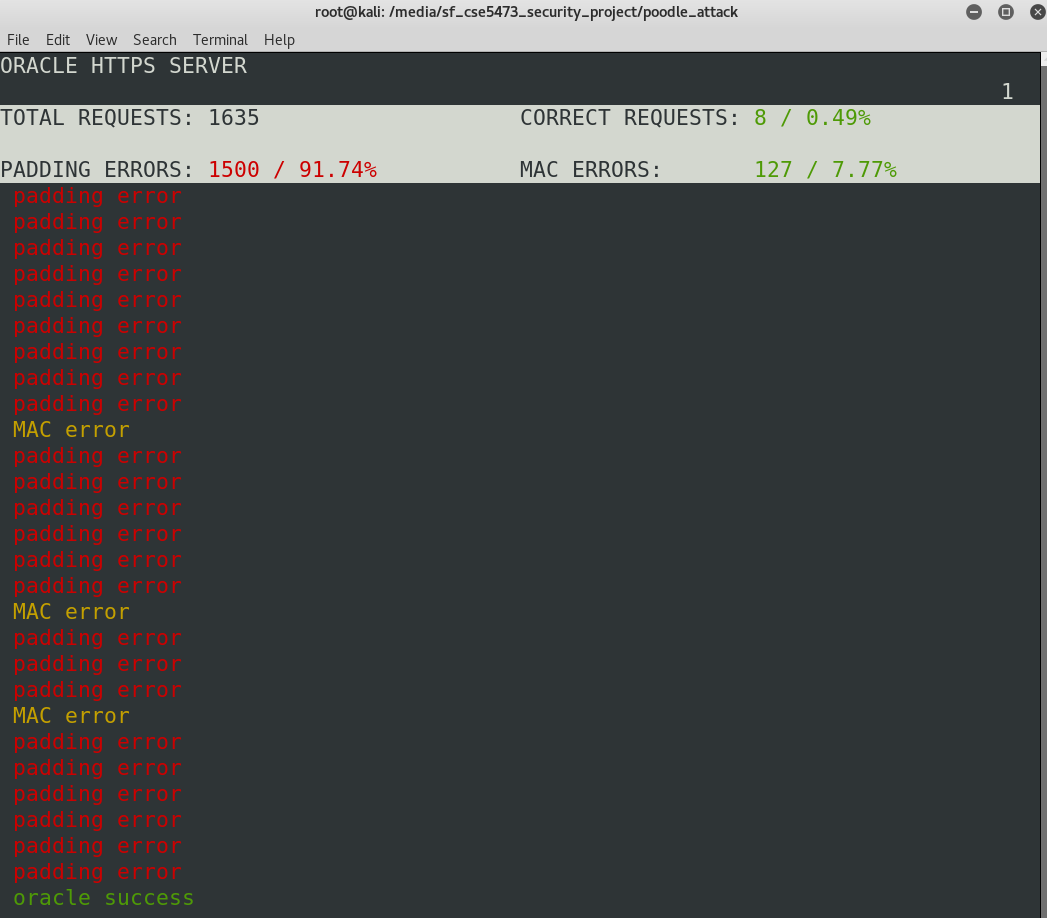
**Key Attack Steps**

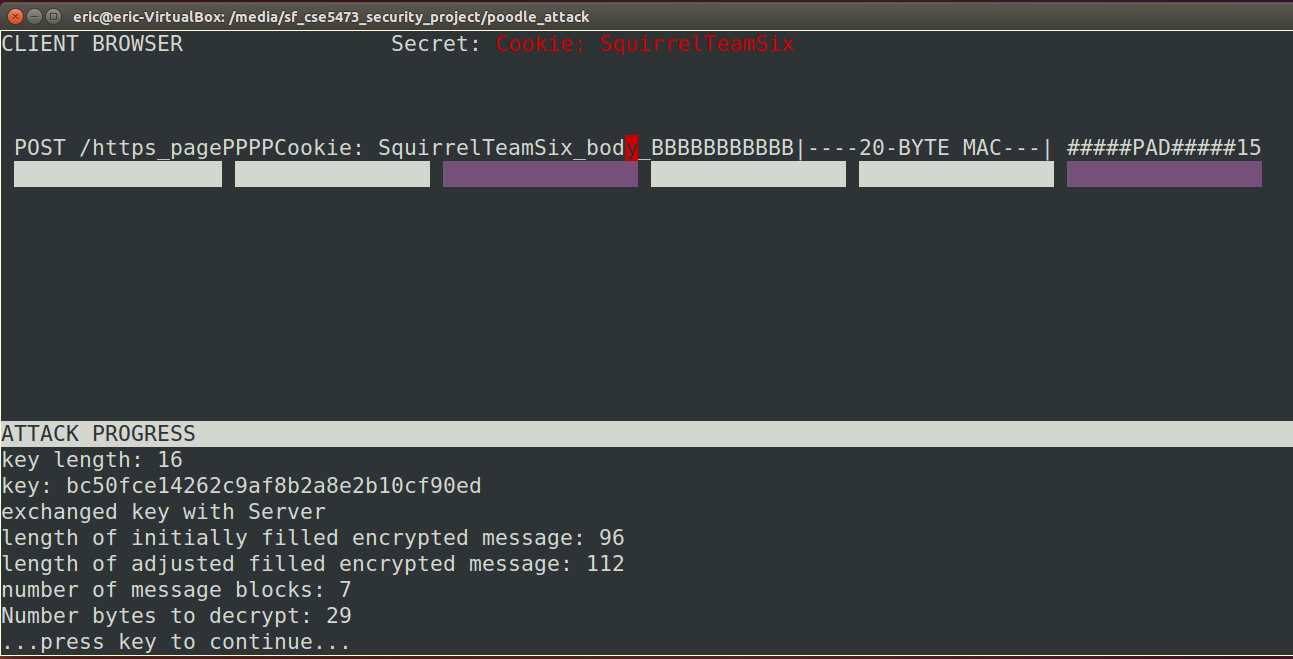
1. Add initial fill bytes to the HTTPS request path and body.
2. Intercept modified encrypted request, C0||C1||...Cn, and continue to add fill bytes to the HTTPS request body until the modified encrypted message increases by a block length. The IV is appended to the encrypted message as C0 from the client.
3. Key concept: now the attacker knows a full block of padding exists in block Cn, with no MAC contamination. This block can be replaced by a block Ci without affecting the MAC.
4. Replace block Cn with block Ci and forward the request to the server oracle.
5. If the server accepts the block with correct padding/correct MAC, the last byte of block Ci can be decrypted (see details in graphic below)
6. If the server rejects the block with incorrect padding/MAC, the attacker triggers the client to re-encrypt the same request. A new IV is used, so the encrypted contents are changed, Cn is again replaced with Ci, and the message is again sent to the server. This process is repeated until the server accepts the block.
7. After decrypting the last byte of Ci, attacker request generator removes one fill byte from the request body, and inserts an additional fill byte to the path. This shifts the cookie/data blocks one byte to the right while maintaining a full block of padding.
8. Repeat steps 4-7 until all of the cookie bytes are decrypted.

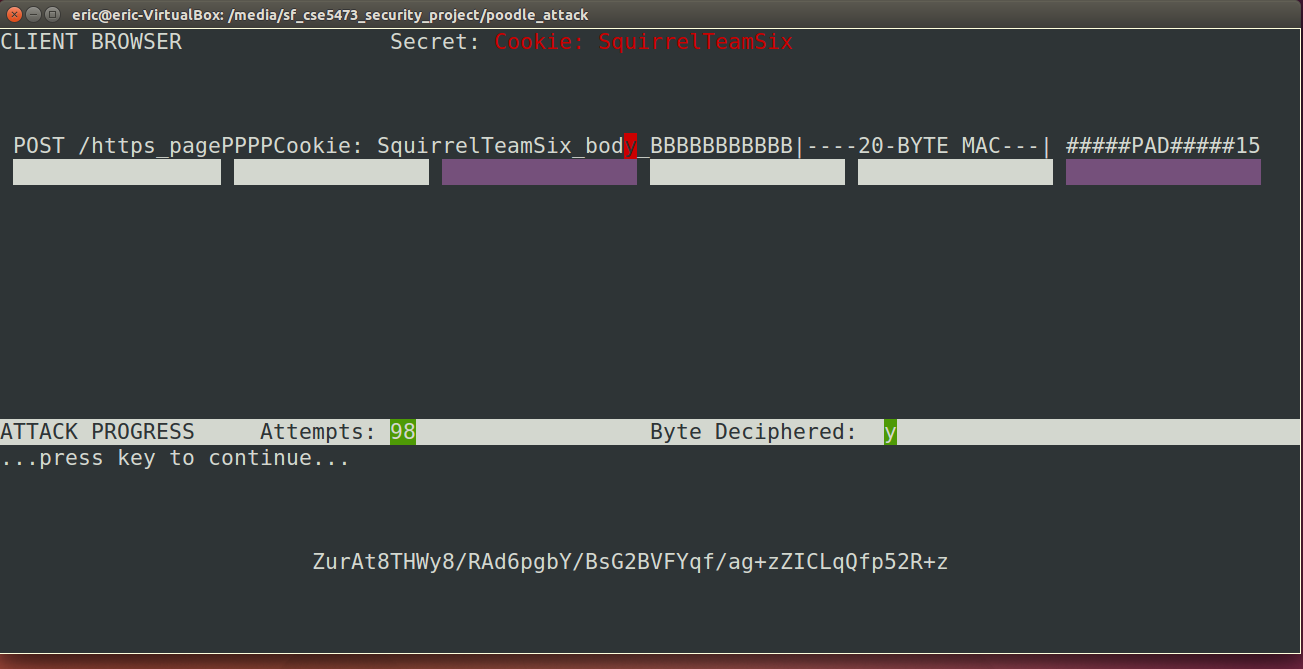
**Low-level attack process visualized** ((graphic from our PowerPoint presentation

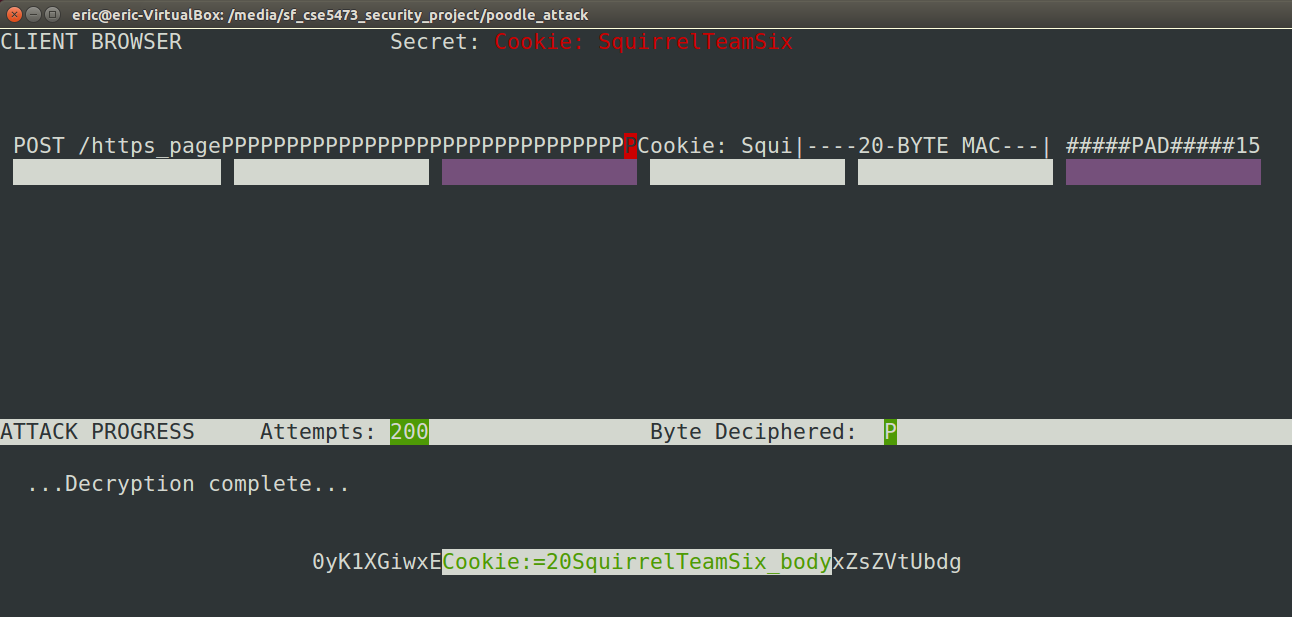


**Our Implementation and Visualization of the Attack and Defense using Curses shell graphics module**







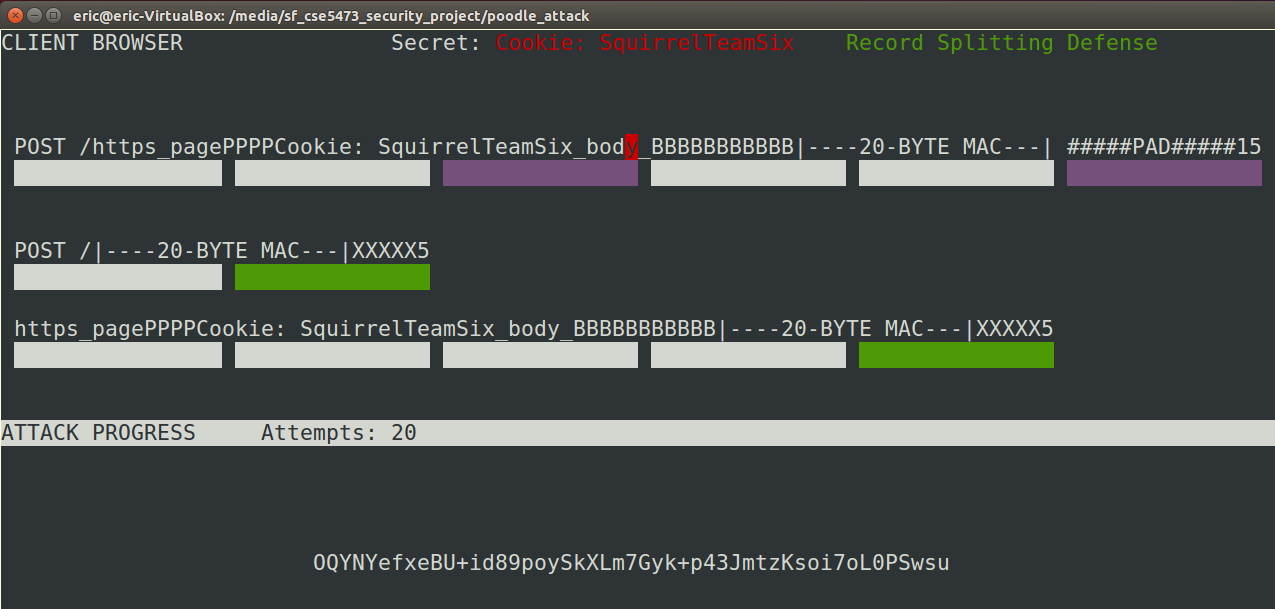


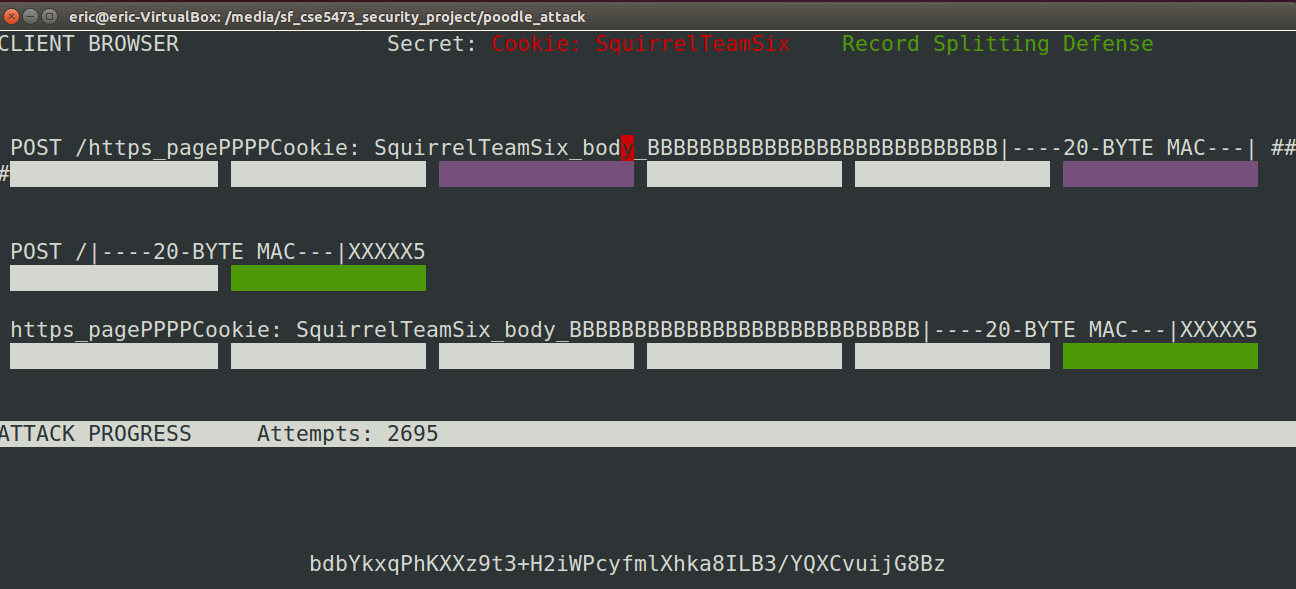
**Defense Proposal & Experiment**

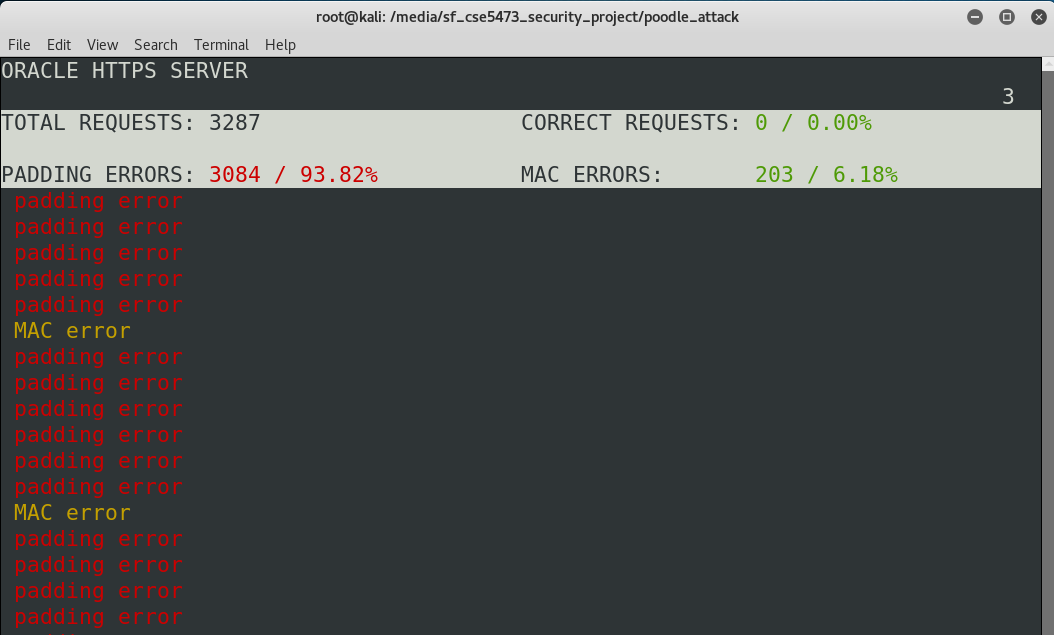
The attack is a very low-effort attack, with a successful response from the server occurring every 1/256 attempts, until an IV / Key combination produce a final padding byte in Ci that is decrypted to a value of 15 (x0F). The Opera browser implemented some temporary anti-POODLE record splitting whose details we didn’t find, but gave us the idea to split vulnerable records before encryption, in order to ensure that a full block of padding would never exist, and that sufficient bytes of the MAC would be pushed into the final block Cn, in order to sufficiently decrease the odds of a successful oracle response.

A 6 / n-6 record splitting approach seems to make intuitive sense, as it pushes 10 bytes of MAC into the final blocks of both split records. A record split would be executed at the browser above the encryption layer anytime that it receives a message length where length(message +MAC) % 16 ==0, i.e. a message that would result in a full block of padding. Upon identifying this condition, the browser splits the record into two records. The first record contains the first 6 bytes of the plaintext message, and the second record contains the remaining n-6 bytes. Both records are then independently MAC’d, padded, and encrypted. The effect is that the 20-byte MAC is pushed into the final message block, so that both messages contain 10 bytes of MAC, and 6 bytes of padding. This now decreases the probability that an attacker can replace the final block and achieve a successful match of both the final byte of padding AND 10 bytes of MAC in the last block from 1/256 to 1/288 = 3.23x10-27. This makes a successful attack much less likely. As seen below, the attacker is not successful after 3,000 oracle requests. Of course the ultimate solution is to disable SSLv3 altogether, as modern browsers have now done, but this record splitting may server as an effective interim solution. This defense approach could be further modified to split records with fewer than X MAC bytes in the final block, say if an attacker attempted to submit records with 15 bytes of padding and a single byte of MAC in the final block in an attempt to avoid a record split, if the cost of a 1/216 oracle success was still an affordable cost of effort.

One of the drawbacks to this defense is that it requires servers to correctly handle assembly of split records upon receipt, which has a non-trivial likelihood of causing interoperability problems between browsers employing a record-splitting defense and servers.







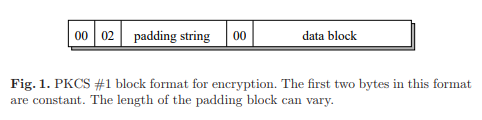
**Bleichenbacher Attack Overview**

The Bleichenbacher attack is an adaptive chosen ciphertext attack against certain protocols based on RSA that was introduced by Daniel Bleichenbacher in 1998. Bleichenbacher shows that an RSA private-key operation can be performed if the attacker has access to an oracle that, for any chosen ciphertext, returns only one bit telling whether the ciphertext corresponds to some unknown block of data encrypted using PKCS #1. SSL V.3.0 is a protocol that is susceptible to this attack.

The attacker uses the oracle to decrypt or sign a message. To do so, the attacker sends ciphertexts to the oracle and by combining the returns from the oracle, the attacker can gain information on cd. The chosen ciphertexts sent to the oracle are based on the previous outcomes of the oracle, which is why the attack is called an adaptive chosen ciphertext attack. This attack is considered to be very practical, as it is easy to get necessary information based on the replies from the oracle. The attack can be carried out if the attacker, for example, has access to a server that accepts encrypted messages and returns an error message depending on whether the decrypted message is PKCS conforming.

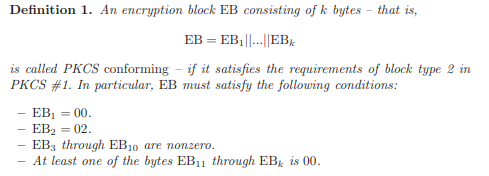
**PKCS #1**

To better understand the attack, the RSA encryption standard PKCS #1 must be described. The standard consists of three block formats, block types 0 and 1, which are reserved for digital signatures, and block type 2 which is used for encryption. Block type 2 is the main block format that is relevant to the attack.



In RSA, n, e are the public key and p, q, d are the secret key. n = pq and d ≡ e−1 (mod ϕ(n)). Furthermore k represents the byte length of n. Hence, we have 28(k−1) ≤ n < 28k. A data block D consists of |D| bytes and is encrypted as follows. The first step is that a padding string PS, which consists of k-3-|D| nonzero bytes is generated pseudo-randomly. The byte length of PS is at least 8, because |D| must not exceed k-11. Thus, the encryption block EB = 00||02||PS||00||D is formed and is converted into an integer x and is encrypted with RSA. This means that the ciphertext c ≡ xe (mod n).

An important aspect to understand is how the receiver parses the ciphertext. By decrypting the ciphertext with the private key, the receiver gets an integer x’. Then x’ is converted into an encryption EB’. From there, the receiver looks for the first zero byte, which indicates the ending of the padding string PS and the start of data block D.



A ciphertext c is PKCS conforming if its decryption is PKCS conforming.

**Chosen-Ciphertext Attacks and Bleichenbacher Attack**

In a basic chosen-ciphertext attack, the attacker selects the ciphertext and sends it to the victim. In return the corresponding plaintext or some part thereof is given. The Bleichenbacher attack is called adaptive because unlike a basic chosen-ciphertext attack, the attacker can choose the ciphertexts depending on the previous outcomes of the attack.

Plain RSA is susceptible to a chosen-ciphertext attack because the attacker can choose a random integer s and ask for the decryption of the message c’ = sec mod n. From the answer m’ = (c’)d and it is easy to recover the original message due to the fact m = m’s-1 (mod n).

Furthermore, another aspect of RSA encryption is that the least significant bit is as secure as the whole message. This means that if there exists an algorithm that can predict the least significant bit of a message given only the corresponding ciphertext and public key, then there is an algorithm that can decrypt a ciphertext. Thus an attacker does not need to learn the complete decrypted message in a chosen-ciphertext attack, but instead can rely on decrypting single bits per chosen ciphertext.

For the Bleichenbacher attack, it is assumed that the attacker has access to an oracle, which returns whether the corresponding plaintext is PKCS conforming for every ciphertext. The Bleichenbacher attack’s goal is to minimize the number of chosen ciphertexts and wants to take advantage of the specific properties of PKCS #1. The main aspect that the attack relies on is that the first 2 bytes of the PKCS #1 format are constant and that these two bytes are known with certainty when a ciphertext is accepted.

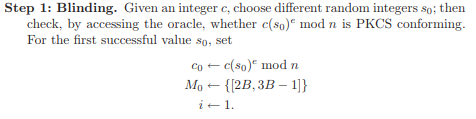
**Description of Bleichenbacher Attack**

The attacker wants to find m = cd (mod n), where c is an arbitrary integer. Basically, the attacker chooses integers s and computes c’ = cse (mod n) and sends c’ to the oracle. The oracle will then determine if c’ is PKCS conforming and if the oracle says that c’ is PKCS conforming, then the attacker knows that the first two bytes of ms are 00 and 02. Furthermore, we know B = 28(k-2) and k is the length of n in bytes. This means that if ms is PKCS conforming, then we know 2B ≤ ms mod n < 3B.

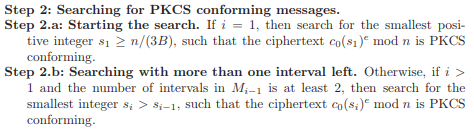
m can eventually be derived by collecting several such pieces of information. About 220 chosen ciphertexts will be sufficient to derive m.

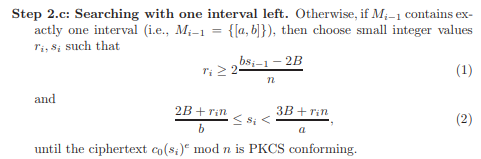
Bleichenbacher describes the attack in 3 phases, where the variable Mi will always be a set of closed intervals that is computed after a successful si has been found, such that m0 is contained in one of the intervals of Mi.

The first phase consists of the message being blinded, where a ciphertext c0 that corresponds to an unknown message m0 is given.

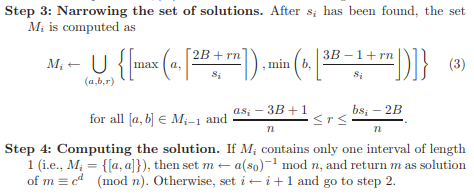


For the second phase, the attacker will try to find small values si, for which the ciphertext c0(si)e mod n is PKCS conforming. For each successful value of si, the attacker will compute a set of intervals that must contain m0 using previous knowledge about m0.

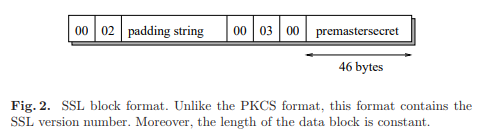




When one interval remains, the third phase begins. The attacker at this point has sufficient information about m0 to choose si, such that c0(si)e mod n is much more likely to be PKCS conforming than is a randomly chosen message. The size of si is increased gradually, which narrows the possible range of m0 until only one possible value remains.



**SSL V.3.0**



SSL V.3.0 is susceptible to the Bleichenbacher attack during the SSL V.3.0’s handshake protocol. When the client and server first exchange the client.hello and server.hello messages, which among other information exchanges, the cryptographic routines are selected. After that, the client and server may send their public key and certificates. The client will then generate a random secret bit string, which is called the pre\_master\_secret, which is encryted with RSA and the resulting ciphertext is sent to the server, which decrypts the ciphertext. If the server finds that the resulting plaintext from the decrypted ciphertext is not PKCS conforming, the server will send an alert message to the client and will close the connection. Otherwise, if the resulting plaintext is PKCS conforming, the server will continue the handshake protocol. The client then will send a finished message, which contains strong authentication and the client will need to know the pre\_master\_secret to compute the message.

An attacker cannot complete the handshake protocol successfully without being able to generate a finished message based on the pre\_master\_secret. However, the attacker does not have to complete the handshake protocol because the attacker gets the necessary information, whether the chosen message is PKCS conforming before the protocol is finished. Thus, by constantly checking if the chosen messages are PKCS conforming, the attacker gradually learns more and is able to determine the original message of the client.

**References**

This POODLE Bites: Exploiting The SSL 3.0 Fallback, https://www.openssl.org/~bodo/ssl-poodle.pdf

POODLE attacks on SSLv3 (14 Oct 2014), Imperial Violet blog, https://www.imperialviolet.org/2014/10/14/poodle.html

[BEAST] T. Duong, J. Rizzo: “Here Come The ⊕ Ninjas”, 2011.

Bleichenbacher, Daniel (1998). ["Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1"](https://web.archive.org/web/20120204040056/http:/www.bell-labs.com/user/bleichen/papers/pkcs.ps). *CRYPTO '98*: 1–12. Archived from [the original](http://www.bell-labs.com/user/bleichen/papers/pkcs.ps) (PS) on 2012-02-04. Retrieved 2011-12-07