PhD First Year Report: Information Leakage on Encrypted Sensor Network Traffic

Yan Yan

May 13, 2015

Contents

Chapter 1

Introduction

1.1 Cryptography and Side Channel Attacks

Cryptography derived from solving the problem of transmitting secret information through an insecure channel. The general principle in modern cryptography is that the encryption and decryption algorithms are assumed to be made public and the secrecy of messages is solely relied on the secrecy of the key.

Under this assumption, cryptographic algorithms are then designed in various ways. Some of them are derived from hard mathematical problems such as Discrete Logarithm and Elliptic Curves. Provable Security provides mathematical proofs by modelling the algorithms in an abstracted mathematical world and reduces them to hard problems; the secrecy of message is then guaranteed as long as the underlying mathematical problems are not solved.

However, when implemented in real world things can get out of control. Many factors considered difficult to be modelled mathematically can sometimes be exploited to breach the security. For example, [1] describes a method called Differential Power Analysis which recovers the secret key using power traces measured during encryption; [2] and [3] shows that the timing information can also reveal the secret key.

1.2 Network Traffic

The conceptional structure of today's network is described in [4]. Generally speaking, networks are formed by protocols which are standard agreements implemented by nodes connected to the networks. Protocols are categorised as a stack of layer with the lower ones handle the fussy transportation problems and the higher ones the more sophisticated functional problems.

Packet (or frame) is the unit of structured data transmitted through network at

each layer. A typical format of packet is a protocol header followed by its payload. The header constitutes of several fields which contain some meta data of the packet while the payload is the actual data being transmitted.

	Layer	Example Protocols
High	Application Layer	HTTP / SMTP / NTP
	Secure Layer	TLS / SSL / DTLS
	Transport Layer	TCP / UDP / SCTP
	Network Layer	IPv4 / IPv6 / 6lowPAN
	Data Link Layer	IEEE 802.3 / IEEE 802.11
Low	Physical Layer	Bluetooth / DSL

Table 1.1: A Simplified 6 Layer Model

Packet of protocols are organised recursively, i.e. headers of upper protocols is embedded into the payload of lower protocols. When a packet (or frame) arrives a node on the network, the headers are decapsulated sequentially from the lowest layer to the highest. Conceptional speaking, the content of a payload should be transparent to the protocols beneath. For instance, a router may only decapsulate a packet no higher than IP layer and has no concern about everything above.

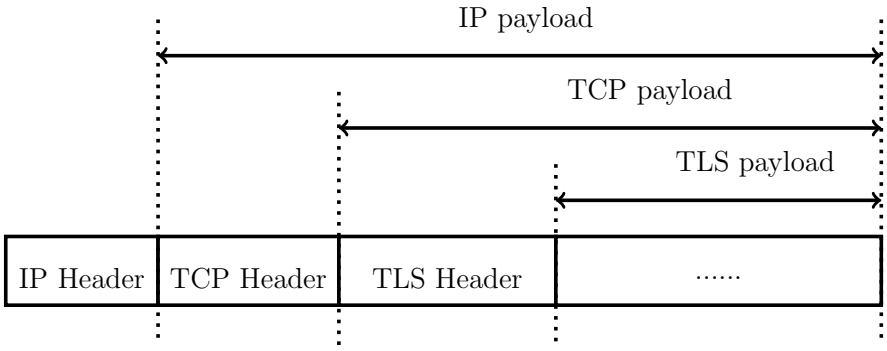

Figure 1.1: An example of headers and payloads

It might be difficult in real world to prevent a third party from seeing a packet. For example, a packet from your laptop cannot reach Google server without hopping between routers and hence any corrupted router may breach the data; the enriching application of mobile devices made it even more difficult as the radio signals from one's smart phone can be captured easily in a cafe.

1.3 Side Channel Information in Packets

Theoretically speaking, encryption can be applied at any layer of a network. Lower the layer it is, more information is protected. However, the intense requirement of efficiency and bandwidth have limited the usage of cryptography, like IPSec. A trade-off between security and efficiency must be made and encryption at higher level protocol has eventuall adopted as a widely accepted solution. As a result, TLS/SSL has became the most used security protocol on Internet today.

The drawback, as mentioned above, is that all headers in the lower layers will be transmitted in plaintext. Figure 1.2 is an example of a captured DTLS packet.

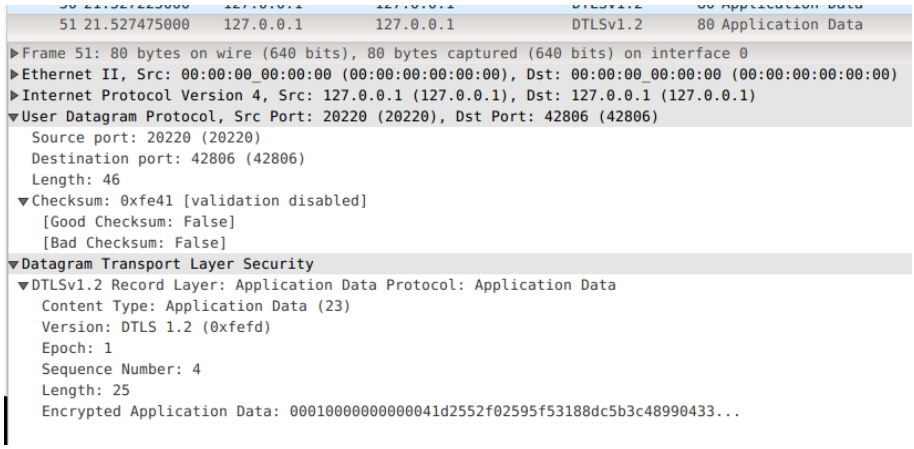

Figure 1.2: A Wireshark Screenshot

As we can see in Figure 1.2, although the sniffer is not able to decrypt the packet, all headers until DTLS are indeed accessible.

1.4 Motivation and Challenges

The open nature of the development Internet of Things (IoT) demands more security and privacy measure. Unlike the stable and already-widely-deployed Internet, the structure of IoT network is still under a developing process; therefore it might be worthwhile to take into concern the security from an early stage.

One challenge in this project is the fundamental nature difference between network traffic and other physical side channel information. Many side channel attacks are aimed to recover secret key materials, such as DPA in [1], or Cache-timing Attack in [2] and [3].

Although it is not certain at this stage that whether there is a link between the value of cryptographic key chosen and packet headers, but intuitively they are more likely to be independent. The reason is that the cryptography primitives chosen should only affect the value of ciphertext which constitutes the payload; hence is expected to be transparent to the lower layer protocol headers. However, the timing information might still be exploited to recover the key material.

Different protocol suite result into different headers and hence different information. As a beginning for this project, we choose to study the traffic generated by a DTLS implementation called tinyDTLS[5]. tinyDTLS is designed to be suitable for embedded systems and is one of the IoT candidates in the future.

Chapter 2

Literature Review

2.1 Academic Publications

[6] demonstrated that this kind of leakage indeed exists in some web applications. Firstly, different web page has different page sizes; thus the size can be exploited as a fingerprint to indicate which page the victim accessed. Secondly, on some pages where part of its content is generated dynamically, such as suggestions in a search box, the size of the dynamic content can again be used as a fingerprint and therefore reveal the victim's input which is supposed to be kept secret.

[7] focuses on detecting leakage points of input in web applications. In this paper, a web applications is modelled as a finite state machine. Observable packet information, such as length and flags in a TCP header, are represented as a vector. A trace is then defined as a sequence of packet information. The leakage points are then measured by estimating the mutual information of the input and each point in the trace. As an extension to mutual information analysis, [8] and [9] provide methods to improve accuracy and performance of the test.

[6] and [7] together lay a foundation to this project. [6] focuses more on the fact that information leakage through encrypted network traffic actually exists but the attacks it describes are relatively web-site specific, although this could be a feature in this subject. The mutual information test proposed in [7] is a powerful tool to pinpoint the leakage points but it also suffers from a performance issue as it requires a huge amount of computation.

[10] and [11] described two actual attacks using packet length. [10] uses packet length to fingerprint pages which contains potentially privacy information. [11] attacks search keyword by profiling the size of response for each character typed in the search box, then matches the victim's traffic in a suffix tree built for the dictionary by a stochastic algorithm.

Packet length might be the most juicy target in packet analysis attacks. These are particularly efficient and requires only passive observation and not much effective countermeasures are proposed. However, the effectiveness of these attacks might be affected by divergence of packet lengths which can be seen common as a result of ads or other kinds of dynamic contents in web pages. One potential problem in [11] is that the profiling step takes a long time due to the response time of search engine and the dictionary chosen also has a great impact on the efficiency and accuracy of attack. It might be worthy pointing out that most theoretical cryptographical research studies only secrecy of plaintexts with same length which is not the case in real world. I personally think that these attacks exploited a blind spot in theoretic study and have displayed the gap between theoretical world and practical world. Packet length is also the most studied side channel information in our experiment at this stage. (See Chapter 3)

Compression ratio obtained by toggling the compress flag in some protocol can also be exploited to recover plaintext. The general idea of this kind of attack is described in [12]. This attack requires the adversary being able to inject his guesses of plaintext into the uncompressed plaintext. The compression ratio will be relatively higher when the guess matches part of the plaintext and lower if it does not. [13] and [14] gave implementations against TLS and HTTPS in real scenarios respectively. [15] proposed some countermeasures by disabling compression or inducing some length hiding mechanism.

At a first glance, the partial plaintext control assumption in [12] seems to be weird, but [14] has demonstrated that such circumstances can be practically achieved by a phishing link. Further more, some crucial information can be attacked such as the session cookie which can then be used to hijack a https session, like on-line banking. As an impact of these attacks, the latest TLS standard has disabled the usage of compression. Nevertheless, when it comes to constrained environment where bandwidth becomes precious, a solution better than totally forbidden is desired. However, there is no compression in our current set up(see Chapter 3). This kind of attack is not considered at this stage.

[16] exploits the padding scheme of CBC mode[1] to recover the plaintext. This attack is based on the fact that some SSL implementation returns different error messages on padding error and MAC failure. Since the padding verification is done after decryption but before MAC verification, the adversary can send to the server a partially modified ciphertext and recover the plaintext by different error messages. Although one countermeasure against this attack is to unify the error messages, [17] states that it is still possible to distinguish these errors by measuring the time differ-

[1] `http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_Block_Chaining_.28CBC.29`

ence induced by whether a MAC verification is performed.

The countermeasure against the attack in [16] has been adopted in many recent implementations by unifying the error message. The attack described [17] relies on the heartbeat being turned on and is very sensitive to network latency. Above that as stated in the paper that adding a idle time before respond can effectively prevent this attack. For a sensor network, the time resolution is expected to be higher due to the low processing power of devices. It is not clear at this stage whether this will raise the risk of this attack. However, the cipher suite adopted by our current experimental environment does not have any padding at all(see Chapter 3); hence this kind of attack is not being considered at this stage.

2.2 Standard Specifications

Another part of the related literatures are the RFC specifications[2]. As of this project, we tend to put our focus on the protocols from Network Layer to Secure Layer in Table 1.1 as a consideration of generality. Therefore, the following documents can be regarded as main references of protocol specifications:

- RFC 791[18] is the IPv4 specification. IPv4 is the most widely deployed protocol today. Even though its successor IPv6 has been proposed for more than a decade, the replacing process is taking place very slowly. It is expected that IPv4 will remain its dominance over the next few years.

- RFC 2460[19] is the IPv6 specification. IPv6 is the successor of IPv4. It was published in 1998 due to the exhaustion of IPv4 address. Although kernels today usually support both IPv4 and IPv6, many applications are still based on IPv4. However, as a "next generation" network, many IoT manufacturers also have the trend of adopting IPv6 as their standard.

- RFC 6282[20] is the specification for 6lowPAN. 6lowPAN is a compression header format for IPv6. It is designed for applications over constrained environments such as sensor networks where the resources, like bandwidth, are very limited. Comparing to a standard IPv6 header, a 6lowPAN header omits some fields by setting them to a default value suitable for constrained environments and hence saved some bandwidth as well as processing time.

- RFC 6347[21] is the DTLS specification. DTLS is the counterpart of TLS over UDP. Since DTLS relies on UDP instead of TCP therefore it is considered to be more lightweight but unreliable. Even though UDP is designed to be

[2] `http://www.ietf.org/rfc.html`

connectionless in order to reduce its overhead, DTLS additionally (comparing to TLS) implemented some connection-oriented feature such as sequence to remain functional.

- RFC 7252[22] is the specification document for Constrained Application Protocol, CoAP. CoAP is a general application protocol for constrained environment. It has a similar design to HTTP which has a Request-Respond model and supports methods including GET, POST, PUT and DELETE. CoAP is designed to be able to map to HTTP for interoperability purpose.

Chapter 3

Progress To Date

As a beginning of this project, our first step is to demonstrate that information leakage similar to those described in [6] can be found when the underlying protocol is switched DTLS. The reason is that DTLS is more suitable to sensor networks comparing to TLS due to is relatively lightweight-ness.

The basic idea is to build some toy applications which model typical sensor network traffic generated through DTLS. The information leakage of toy applications are intentionally crafted to emphasise their existence.

Even though both OpenSSL and GnuSSL have DTLS implemented with general features, we setted our experimental the less featured tinyDTLS[5] due to its lightweight-ness, which is more suitable to sensor networks. However, the drawback is that only one cipher-suite, TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8[23], is available for the current version of tinyDTLS. This implies that there should be no padding scheme adopted and hence the length of plaintext and ciphertext are expected to have a linear relationship. Our experiments supported this conjecture such that:

$$l_D = 17 + l \tag{3.1}$$

where l is the length of plaintext and l_D is the value in DTLS length field. According to the specifications the additional bytes is supposed to be purely a resulted of the appending MAC even though 17 bytes is a value unlikely to be. This problem is still under investigating.

All experiments are done with only two processes, a server and a client referred as SERVER and CLIENT, on a same linux host connected through local-link. The protocol suite we adopted is [IPv4 or IPv6] + UDP + DTLS. The modelled adversary is simply a passive eavesdropper.

So far we have built up two toy applications, **Odd or Even** and **Leaky Coffee**, which will be explained in the next sessions alongside with corresponding traffic analysis.

3.1 Odd or Even

Odd or Even is a simple toy application designed to demonstrate the fundamental idea of encrypted traffic analysis.

3.1.1 Application Description

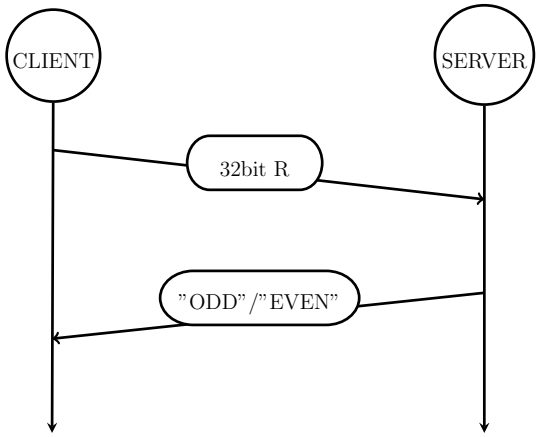

Figure 3.1: Description of an Odd-or-Even session

CLIENT randomly generates a 32-bit unsigned integer R and sends it to SERVER in binary. SERVER replies with a string "ODD" or "EVEN" according to the value of the 32-bit R(Figure 3.1).

3.1.2 Analysis

We run the application for multiple times and collected the packets it generated. As we have expected, "ODD" packets are 1 byte shorter than "EVEN" packets which implies that an eavesdropping adversary can learn what has been sent from SERVER to CLIENT simply by looking at the packets length. However, no obvious leakage has been found in other fields of the packets.

3.2 Leaky Coffee

3.2.1 Application Description

Leaky Coffee simulates a more complicated scenario where the CLIENT sends a coffee order (in string) to SERVER. SERVER echoes the order appended by some

flavour (in string). CLIENT compares the amount of given flavour to an internally generated random requirement and asks SERVER again for more additive if it is insufficient.

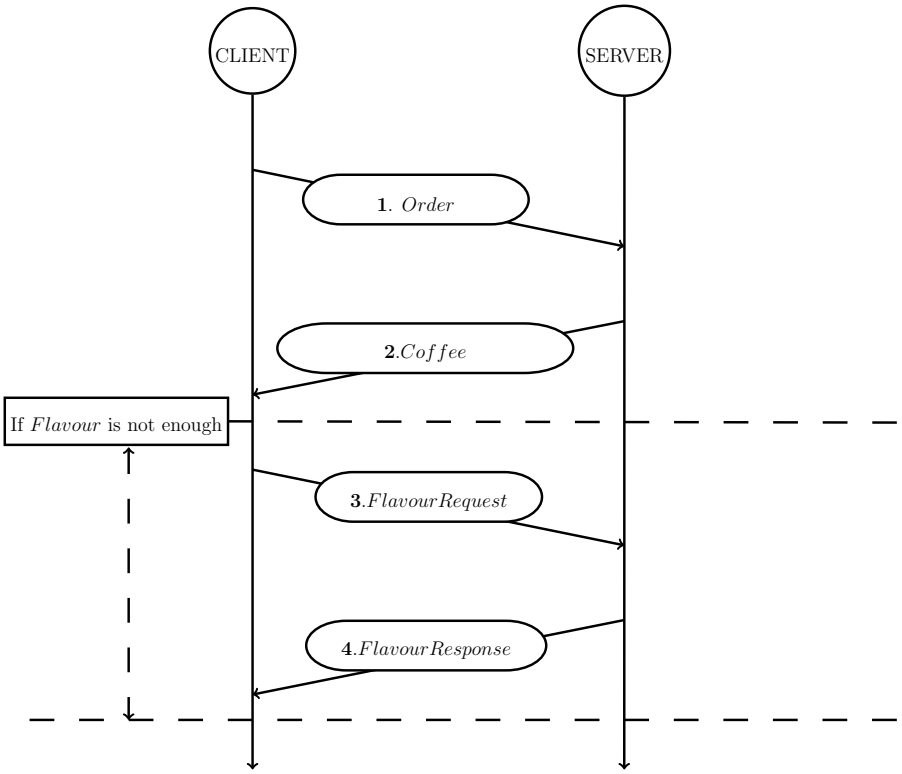

Figure 3.2: Description of a **Leaky Coffee** session

Figure 3.2 describes the procedure of a **Leaky Coffee** session. Example 3.2.1 and Example 3.2.2 are two examples for a 2 packets and a 4 packets session respectively.

Syntaxes

"$A||B$" represents "String A concatenated by string B".
"$|A|$" represents the length of string A.

Definition 3.2.1. $Order$ is an ASCII string randomly selected as:

$$Order = \text{“AMERICANO”}|\text{“CAPPUCCINO”}|\text{“ESPRESSO”}|\text{“MOCHA”}$$

Definition 3.2.2. $Coffee$ is an ASCII string constructed by three substrings: $Order||Milk||Sugar$. $Order$ is defined in Definition 3.2.1. $Milk$ and $Sugar$ are composed of no more than

3 '@' and '*' respectively:

$$Coffee = Order||Milk||Sugar$$
$$Milk = \{\text{'@'}\}^{\{0,3\}}$$
$$Sugar = \{\text{'*'}\}^{\{0,3\}}$$

Definition 3.2.3. *FlavourRequest* is an ASCII string begins with "FLAVOUR" and followed by a $Milk$ then a $Sugar$ defined in Definition 3.2.2.

$$FlavourRequest = \text{"FLAVOUR"}||Milk||Sugar$$

Definition 3.2.4. *FlavourResponse* is identical to *FlavourRequest* defined in Definition 3.2.3.

$$FlavourReponse = FlavourRequest = \text{"FLAVOUR"}||Milk||Sugar$$

Definition 3.2.5. Leaky Coffee Session

A **Leaky Coffee** session performs under the following procedure:

1. CLIENT randomly picks an $Order$(Definition 3.2.1) and sends it to SERVER.
2. SERVER replies to CLIENT with a $Coffee$(Definition 3.2.2) where the first part is identical to the $Order$ received. If the $Order$ is "ESPRESSO" then $Milk$ and $Sugar$ are set to be NULL string; otherwise they are generated randomly.
3. If $Coffee$ is "ESPRESSO" then the session is completed; otherwise CLIENT compares $|Milk|$ and $|Sugar|$ with two random integer selected from $[0, 3]$ by itself. If any of them are smaller than the integer, then CLIENT sends out a $FlavourRequest$(Definition 3.2.3) with its $Milk$ and $Sugar$ corresponds to the insufficient part.
4. Upon receving a $FlavourRequest$, SERVER sends back a $FlavourResponse$(Definition 3.2.4) that is identical to the $FlavourRequest$ it received.
5. CLIENT randomly sleeps for 5 to 10 seconds before re-initiates another **Leaky Coffee** session.

In current implementation, all random values are generated **uniformly**.

Leaky Coffee session examples

As in Definition 3.2.5, $FlavourRequest$ and $FlavourResponse$ only appears when $Sugar$ and/or $Milk$ are insufficient in $Coffee$; therefore **Leaky Coffee** sessions can be categorised by the existence of $FlavourRequest$ and $FlavourResponse$.

Example 3.2.1. An example with $FlavourRequest$ and $FlavourResponse$(Figure 3.3)

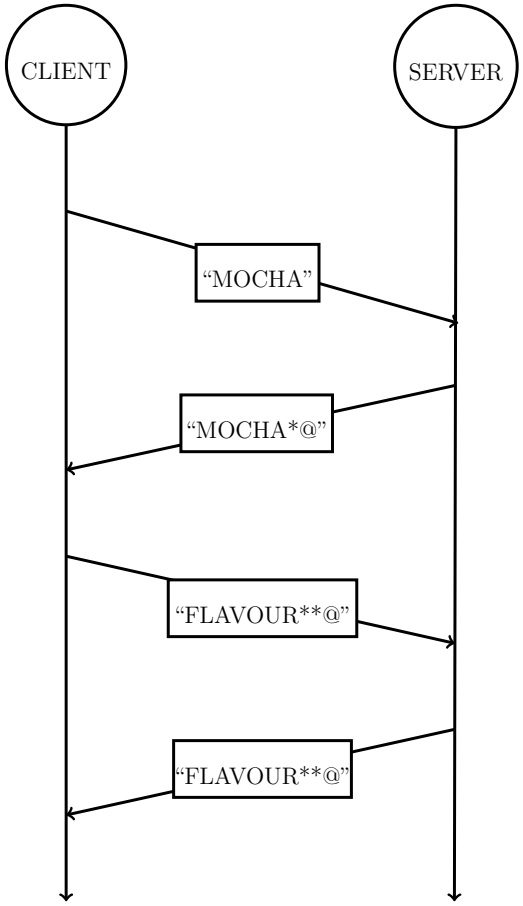

Figure 3.3: Example: A **Leaky Coffee** session with $FlavourRequest$ and $FlavourResponse$

Example 3.2.2. Another example without $FlavourRequest$ and $FlavourResponse$(Figure 3.4):

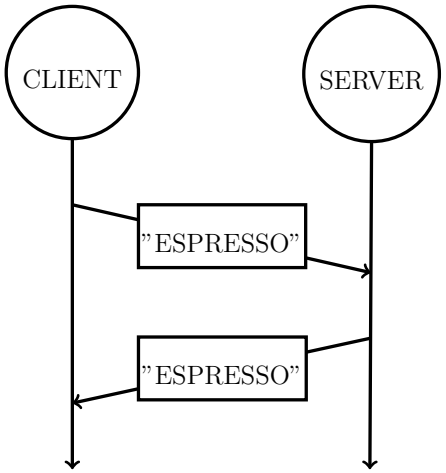

Figure 3.4: Example: A **Leaky Coffee** session without $FlavourRequest$ and $FlavourResponse$

3.2.2 Analysis

Similar to most cryptography researches, we assume the implementation of **Leaky Coffee** are made public. We model our adversary to be given the full knowledge that is observable through a sniffer[1], as those displayed in Figure 3.5.

[1]In this project, we used Wireshark[24].

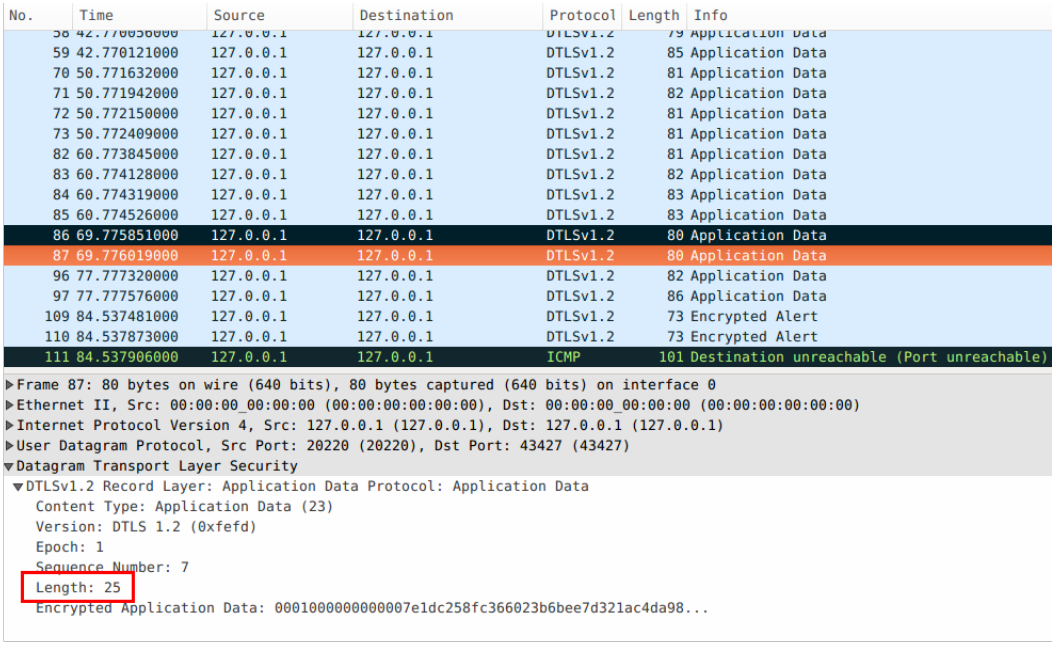

Figure 3.5: Captured Leaky Coffee packets

3.2.3 Session Detection and Segmentation

The existence of packets implies that a session is taking place between CLIENT and SERVER.

Further more, since there is a significant difference in the timestamp intervals between continuous packets from same session and different session, one can group packets by their timestamps. Typically a threshold of 4 seconds is good enough for **Leaky Coffee**. As we can see in the "Time" column in Figure 3.5[2],

- Packet 70 to 73 is a session with $FlavourRequest$ and $FlavourResponse$.
- Packet 82 to 85 is another session with $FlavourRequest$ and $FlavourResponse$.
- Packet 86 and 87 is a session without $FlavourRequest$ and $FlavourResponse$.
- Packet 96 and 97 is another session without $FlavourRequest$ and $FlavourResponse$.
- ...

Once a session has been segmented, we can immediately label them as described in Definition 3.2.5.

[2]The in-continuous packet number is a result for filtering DTLS packets on the hosting machine.

However, timing information could be strongly affected by the environment; therefore the time difference threshold for a real sensor network packets could be different, even hard to define.

3.2.4 Plaintext Guessing

Similar to **Odd or Even**(Section 3.1), ciphertexts exchanged in **Leaky Coffee** has distinguish length which could possibly be exploited to recover the plaintexts.

To formalise it, we model the leakage through ciphertext lengths as a channel[25], inspired by [7]. The general idea is to view the ciphtertext lengths as an input and plaintext the output, then the leakage problem is immediately equivalent to the decoding problem of such a channel.

In order to do this, we first construct a **Forward Channel** that "encodes" plaintexts to ciphertext lengths. The **Leakage Channel**, which "decodes" ciphertext lengths to plaintexts, is therefore followed by as the reversion of **Forward Channel**.

Definition 3.2.6. Let $\mathbb{X}$ be the set of possible plaintexts and $\mathbb{Y}$ the set of possible packet lengths in bytes. The **Forward Channel** is then given as $\mathbf{W}(\mathbf{y}|\mathbf{x})$ and **Leakage Channel** as $\mathbf{W^{-1}}(\mathbf{x}|\mathbf{y})$ where both $x \in \mathbb{X}$ and $y \in \mathbb{Y}$.

Example 3.2.3 describes an example of how Forward Channel and Leakage Channel are constructed.

Example 3.2.3. Take *Order* for example. According to Definition 3.2.1, we have:

$$\mathbb{X} = \{\text{“AMECINANO”}, \text{“CAPPUCINO”}, \text{“MOCHA”}, \text{“ESPRESSO”}\}$$

Hence the Forward Channel is as Table 3.1.

$W(y\|x)$	5	8	9	$P(X = x)$
“AMERICANO”			1	1/4
“CAPPUCINO”			1	1/4
“MOCHA”	1			1/4
“ESPRESSO”		1		1/4

Table 3.1: Forward Channel for *Order*

The ciphertext length is fixed once the plaintext is given; therefore the probability of a ciphertext length could either be 0 or 1.

The joint probability immediately follows by:

$$(\widehat{WP})(x, y) = P(x)W(y|x) \tag{3.2}$$

Which results into Table 3.2.

$\widehat{W}P$	P
("AMERICANO",9)	1/4
("CAPPUCINO",9)	1/4
("MOCHA",5)	1/4
("ESPRESSO",8)	1/4

Table 3.2: Joint Probability of $(\mathbb{X}, \mathbb{Y})$ for *Order*

Since the events of each $X = x$ are exclusive, the marginal probability of $Y = y$ is the sum of each of its joint probabilities:

$$P(Y = y) = \sum_{x \in \mathbb{X}} \widehat{W}P(x, y) \tag{3.3}$$

The result is shown in Table 3.3.

y	$P(Y = y)$
5	1/4
8	1/4
9	1/2

Table 3.3: Marginal probabilities of y for *Order*

Finally we can construct the Leakage Channel using Bayes' theorem:

$$P(x|y) = \frac{P(x)P(y|x)}{P(y)} \tag{3.4}$$

And constrcut the Leakage Channel as shown in Table 3.4

$W^{-1}(x\|y)$	"AMERICANO"	"CAPPUCINO"	"ESPRESSO"	"MOCHA"
5				1
8			1	
9	1/2	1/2		

Table 3.4: Leakage Channel for *Order*

The Leakage Channel(Table 3.4) can be then used as a guideline for an eavesdropper adversary to recover the plaintext being transmitted.

In fact as an implementation optimisation of this method, one can directly construct the Leakage Channel by iterating through each column of the Forward Channel without storing the intermediate tables, as described in Algorithm 1.

Algorithm 1: FC2LC

Input:
Marginal probabilities $P(X = x)$;
Forward Channel $W(y|x)$, where $W_{ij} = P(Y = y_j|X = x_i)$, $i \in |\mathbb{X}|, y \in |\mathbb{Y}|$
Output:
Leakage Channel $W^{-1}(x|y)$ where $W^{-1}_{ji} = P(X = x_i|Y = y_j)$, $i \in |\mathbb{X}|, y \in |\mathbb{Y}|$

begin
  // Iterate over each column of $W(y|x)$
  for $j = 0$; $j < |\mathbb{Y}|$; j++ **do**
    // Reset $J[i]$, the joint probability of $P(x = x_i, y = y_j)$
    $J[i] = \vec{0}$;
    // Compute P_y, the marginal probability of $P(Y = y_j)$, by $J[i]$.
    for $P_y = 0, i = 0$; $i < |\mathbb{X}|$; $i++$ **do**
      $J_y[i] = W_{ij} * P(X = x_i)$;
      $P_y \mathrel{+}= J_y[i]$;
    end
    // Compute $W^{-1}(x|y)$
    for $i = 0$; $i < |\mathbb{X}|$; $i++$ **do**
      $W^{-1}_{ji} = J[i]/\ P_y$;
    end
  end
  return $W^{-1}(x|y)$;
end

One underlining problem in this method is the need to enumerate the plaintext. In some scenarios, it is possible to mitigate this problem by reducing the size of $\mathbb{X}$ by wrapping plaintexts. The cost of such mitigation is the loss of resolution in the recovered plaintext, as shown in Example 3.2.4.

Example 3.2.4. $Coffee$(Definition 3.2.2) is relatively harder to enumerate as the various combination of $Sugar$ and $Milk$. However, if the adversary aims only to guess the first part, $Order$, then the construction of Leakage Channel can be done much more efficiently by giving up the resolution of distinguishing $Sugar$ and $Milk$.

To be more specifically, the construction of Leakage Channel could be simplified by wrapping the "less important" part, in this example $Sugar$ and $Milk$, of plaintexts.

Since we know the probabilities for $Sugar$ and $Milk$, therefore we can construct Forward Channel as Table 3.5.

$W(y\|x)$	5	6	7	8	9	10	11	12	13	14	15	$P(X=x)$
"AMERICANO"					1/16	1/8	3/16	1/4	3/16	1/8	1/16	1/4
"CAPPUCINO"					1/16	1/8	3/16	1/4	3/16	1/8	1/16	1/4
"MOCHA"	1/16	1/8	3/16	1/4	3/16	1/8	1/16					1/4
"ESPRESSO"				1								1/4

Table 3.5: Forward Channel for $Coffee$

Then the Leakage Channel for $Coffee$ can be obtained by Algorithm 1, as shown in Table 3.6.

$W^{-1}(x\|y)$	"AMERICANO"	"CAPPUCINO"	"ESPRESSO"	"MOCHA"
5				1
6				1
7				1
8			4/5	1/5
9	1/5	1/5	3/5	
10	1/3	1/3	1/3	
11	3/7	3/7	1/7	
12	1/2	1/2		
13	1/2	1/2		
14	1/2	1/2		
15	1/2	1/2		

Table 3.6: Leakage Channel for $Coffee$

To summarise, a Leakage Channel can be constructed by the following steps:

1 Wrap the "unimportant part".(optional)

2 Construct the Forward Channel.

3 Construct the Leakage Channel by Algorithm 1.

3.2.5 Guessing Plaintext Using Joint Packet Length

Chapter 4

Plan

The short term plan is to finish the toy application analysis in Chapter 3. There are these directions in this task:

1. So far we have mainly focused on demonstrating the phenomenon similar to those described in [6] and [7] exists in our set up, but there could possibly be more. For example, it is probably worth study whether it is feasible to deduce the plaintext distribution in Section 3.2 given encrypted packets.

2. To see if the attacks in Section 3.2 can be optimised.

3. Apply and evaluate some countermeasures to these attacks.

4. Only a few, nearly none, attempt has been made to study types of attack other than [6] and [7]; hence this might also be worth trying.

One of the greatest deficiency in the work so far is the risk of being alienated from reality since the toy applications are designed in an extremely abstracted way whilst the real world application could be much more complicated and will not be intentionally designed to be vulnerable to attacks. Therefore as a long term plan, it is very important to get in touch with some actual application and evaluate those we have developed from the toys. Having said so, one of the greatest challenges is the immaturity of IoT; hence following the trend of related technologies would be an important and constant task in this project.

Chapter 5

Other Activities

I have been one of the TAs for Cryptography A and System Security during the first term of 2014 - 2015.

I also attended Real World Crypto 2015.

Bibliography

[1] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks - revealing the secrets of smart cards*. Springer, 2007. ISBN: 978-0-387-30857-9.

[2] Daniel J. Bernstein. "Cache-timing attacks on AES". In: (2004). URL: http://cr.yp.to/papers

[3] Dag Arne Osvik, Adi Shamir, and Eran Tromer. "Cache attacks and Countermeasures: the Case of AES." In: *IACR Cryptology ePrint Archive* 2005 (2005), p. 271. URL: http://dblp.uni-trier.de/db/journals/iacr/iacr2005.html#OsvikST05.

[4] International Organization for Standardization ISO. *ISO/IEC 7498-1Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model*. Tech. rep. June 15, 1994, pp. 34–65+.

[5] *tinyDTLS*. http://tinydtls.sourceforge.net/.

[6] Shuo Chen et al. "Side-Channel Leaks in Web Applications: A Reality Today, a Challenge Tomorrow". In: *31st IEEE Symposium on Security and Privacy, S&P 2010, 16-19 May 2010, Berleley/Oakland, California, USA*. 2010, pp. 191–206. DOI: 10.1109/SP.2010.20. URL: http://doi.ieeecomputersociety.org/10.1109/SP.2010.20.

[7] Luke Mather and Elisabeth Oswald. "Pinpointing side-channel information leaks in web applications". In: *J. Cryptographic Engineering* 2.3 (2012), pp. 161–177. DOI: 10.1007/s13389-012-0036-0. URL: http://dx.doi.org/10.1007/s13389-012-0036-0.

[8] Mário S. Alvim et al. "Measuring Information Leakage Using Generalized Gain Functions". In: *25th IEEE Computer Security Foundations Symposium, CSF 2012, Cambridge, MA, USA, June 25-27, 2012*. 2012, pp. 265–279. DOI: 10.1109/CSF.2012.26. URL: http://doi.ieeecomputersociety.org/10.1109/CSF.2012.26.

[9] Tom Chothia and Apratim Guha. "A Statistical Test for Information Leaks Using Continuous Mutual Information". In: *Proceedings of the 24th IEEE Computer Security Foundations Symposium, CSF 2011, Cernay-la-Ville, France, 27-29 June, 2011*. 2011, pp. 177–190. DOI: 10.1109/CSF.2011.19. URL: http://doi.ieeecomputersociety.org/10.1109/CSF.2011.19.

[10] George Danezis. *Traffic Analysis of the HTTP Protocol over TLS*.

[11] Alexander Schaub et al. "Attacking Suggest Boxes in Web Applications Over HTTPS Using Side-Channel Stochastic Algorithms". In: *IACR Cryptology ePrint Archive* 2014 (2014), p. 959. URL: http://eprint.iacr.org/2014/959.

[12] John Kelsey. "Compression and Information Leakage of Plaintext". In: *Fast Software Encryption, 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002, Revised Papers*. 2002, pp. 263–276. DOI: 10.1007/3-540-45661-9_21. URL: http://dx.doi.org/10.1007/3-540-45661-9_21.

[13] *The CRIME Attack*. https://docs.google.com/presentation/d/11eBmGiHbYcHR9gL5nDyZChlCa2GizeuOfaLU2HOU/edit.

[14] Yoel Gluck, Neal Harris, and Angelo (Angel) Prado. *Breach: Reviving the CRIME Attack*. Tech. rep. 2013. URL: http://breachattack.com/resources/BREACH%20-%20SSL,%20gone%20in%2030%20seconds.pdf.

[15] Janaka Alawatugoda, Douglas Stebila, and Colin Boyd. "Protecting Encrypted Cookies from Compression Side-Channel Attacks". In: *IACR Cryptology ePrint Archive* 2014 (2014), p. 724. URL: http://eprint.iacr.org/2014/724.

[16] Serge Vaudenay. "Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS ..." In: *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*. 2002, pp. 534–546. DOI: 10.1007/3-540-46035-7_35. URL: http://dx.doi.org/10.1007/3-540-46035-7_35.

[17] Nadhem J. AlFardan and Kenneth G. Paterson. "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols". In: *2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013*. 2013, pp. 526–540. DOI: 10.1109/SP.2013.42. URL: http://dx.doi.org/10.1109/SP.2013.42.

[18] J. Postel. *Internet Protocol*. RFC 791 (INTERNET STANDARD). Updated by RFCs 1349, 2474, 6864. Internet Engineering Task Force, Sept. 1981. URL: http://www.ietf.org/rfc/rfc791.txt.

[19] S. Deering and R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*. RFC 2460 (Draft Standard). Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946, 7045, 7112. Internet Engineering Task Force, Dec. 1998. URL: http://www.ietf.org/rfc/rfc2460.txt.

[20] J. Hui and P. Thubert. *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*. RFC 6282 (Proposed Standard). Internet Engineering Task Force, Sept. 2011. URL: http://www.ietf.org/rfc/rfc6282.txt.

[21] E. Rescorla and N. Modadugu. *Datagram Transport Layer Security Version 1.2*. RFC 6347 (Proposed Standard). Internet Engineering Task Force, Jan. 2012. URL: http://www.ietf.org/rfc/rfc6347.txt.

[22] Z. Shelby, K. Hartke, and C. Bormann. *The Constrained Application Protocol (CoAP)*. RFC 7252 (Proposed Standard). Internet Engineering Task Force, June 2014. URL: http://www.ietf.org/rfc/rfc7252.txt.

[23] D. McGrew et al. *AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS*. RFC 7251 (Informational). Internet Engineering Task Force, June 2014. URL: http://www.ietf.org/rfc/rfc7251.txt.

[24] *Wireshark*. https://www.wireshark.org/.

[25] C. E. Shannon. "A Mathematical Theory of Communication". In: *SIGMOBILE Mob. Comput. Commun. Rev.* 5.1 (Jan. 2001), pp. 3–55. ISSN: 1559-1662. DOI: 10.1145/584091.584093. URL: http://doi.acm.org/10.1145/584091.584093.