IDEAS
Internet-Draft
Intended status: Informational
Expires: May 18, 2018

R. Moskowitz
Huawei

November 14, 2017

An Attack on Privacy in Mobile Devices
draft-moskowitz-mobile-privacy-attack-01

Abstract

This memo outlines an attack against the privacy of the Identities of mobile devices with all the IETF secure enveloping technologies. It describes necessary steps to be taken with those technologies, the underlying address assignment strategies, and role of secure 3rd party introducers.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 18, 2018.

Table of Contents

1. Introduction

In recent years there has been a drastic increase of theft of Personal Identifying Information (PII). This has resulted in an increase scrutiny of new work in the IETF, not to add new attack vectors. Most of this attention has been on work associated to people owned devices like mobile computing platforms. It also impacts work on 'machines' that are not operated directly by people, but in the end, owned by people (or corporations).

The privacy concern arises in that along with the PII, the device location information is also stolen. Thus where a person or corporation's devices are is strongly bound to the stolen PII. NATed addresses are also often in the stolen information, as the client applications have been observed to query the OS for the local address and pass that to the server for storage along with the collected PII. No information about the device seems to be safe from harvesting and theft.

This memo will describe a linked, privacy attack, tracing a device through all of its connections to other devices. The attack is pernicious. ALL existing secure communication protocols contribute to the attack. Current IP address allocation practices further compound the attack that can obviate any attack mitigation implemented at higher layers.

2. Terms and Definitions

2.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2.2. Notations

This section will contain notations

2.3. Definitions

TBD

3. The Call ID Privacy Attack

The name, "Call ID", is taken from the process where all connections are identified in some way. These IDs can be collected and linked back to PII.

There are two players in this attack, Mal and Eve. Mal maliciously steals PII from wherever it is kept weakly guarded. He does not have to harvest it from a service provider's records of what devices are on the network. Practically all the information needed is in web sites where users and corporations store information and with that information is the IP address and other identifiers of the device.

Eve is patiently eavesdropping on traffic over the Internet, collecting packet identifying information. Eve sees all the exposed headers in every packet. She may even have tapped into IPFIX flows to simplify her work.

Mal and Eve put their data together and are able to construct all communications, including peer-to-peer ones. Nothing is private to the these two.

4. Identifiers leaked by the Data Channel

All secure data channels (e.g. ESP, SRTP, and TLS) have an Identifier to link the packet to the security information. Eve uses these Identifiers to link seemingly disparate flows together so that changing IP addresses (as the result of a move in the network) does not break her knowledge of whom or what is talking to whom or what.

Identifiers MUST be changed by both parties whenever one party changes its address. Further, all other exposed values, particularly

sequence numbers must be changed from the expected value. For example, the sequence number may be jumped in value a random amount but still within the numbering window specified by the protocol.

One approach to change Identifiers is to treat the agreed upon Identifiers as masters and construct a keyed hash-chain for the actual values sent.

4.1. TLS 1.3 Data Channels

TLS 1.3 may well have made the transition to decoupling separate connection 'pieces' as the devices change addresses. It does this through its key scheduling and other security state management components. Further study will be need to see if all needed decoupling hygenics are followed.

4.2. Unsecured Data Channels

It is important to note that there are unsecure data channels (e.g. ILA, IPnIP, LISP) that make no security claims and leak information that can be linked to PII. It will be a separate exercise to see what can be done to minimize the leakage with them.

5. Identifiers leaked by the Control Channel

Secure control channels (e.g. HIP, IKE, and TLS) carry Identities, often in the clear during some part of the exchange, and Identifiers that link all the packets for the control channel 'session'.

It is close to impossible to protect all Identities in the control channels without opening up some significant DOS attacks. Thus other mitigations will be needed. In some cases, short-term Identities may work. In others a 3rd party Introducer will be needed. Both parties to a control channel could have secure connections to a 3rd party. They would exchange their real Identities over this proxied connection before switching to agreed upon one-time Identities on their real control channel. This shifts the risk to the 3rd party.

The Identifiers in the control channel can be masked just like in a data channel. In some cases, like HIP, special care will be needed either through a physical side channel (e.g. QR codes displayed real time with one-time keys) or a 3rd party Introducer to exchange a key used in the keyed hash-chain.

5.1. Unguarded Diffie-Hellman in Control Channels

TLS 1.3 and IKE make use of an "unguarded" Diffie-Hellman exchange to hide identity information. This is also called opportunistic Diffie-Hellman. There are two risks with this. It can be subject to a Man-in-the-Middle attack and it is a great DDOS tool.

The MITM attack against exposing identities will require more study. There are methods to manage the DDOS attack, but this is not a help for small devices that any extra DH is beyond their processing/ battery capability.

6. 3rd Party Introducer

A trusted, 3rd party Introducer can go a long way to mask information in packets to block Eve. A device would maintain a long-lived secure connection to the Introducer. This connection would be established using some agreed upon Identity for both the Introducer and the device.

Over this secure channel, the device would register Identities, discovery information, and access policies. It is this information that other registered devices would use to 'link up' and then shift to a direct peer connection.

This Introducer would have to take significant steps to defend against Mal, as it holds real information about connected parties. Best practices (e.g. Format Preserving Encryption) can go a long way to defeat Mal.

7. The Role of IP Addresses

Any work to mask the various protocol information discussed above will be defeated if all connections for a device come from a single IP address or a single /64 IPv6 prefix. Eve will be able to link all the devices packets together, and Mal will be able to link some of them to PII and the 'game is over'.

Minimally 2 addresses per device are required. One for device to server with PII and one for peer communications. Since it is hard to know what communication will result in storing traceable information, the more addresses used, the better the level of detachment.

8. IANA Considerations

There is no IANA considerations at this time for this document.

9. Security Considerations

This document details a privacy attack and some efforts to mitigate the attack. These efforts could be for naught if the basic provider mapping of devices to access authentication is stolen by Mal.

Further, MAC address harvesting is not discussed. This could potentially be a more serious weakness that IP addresses. Web servers should NOT store any MAC addresses collected from attached clients.

10. Acknowledgments

This attack was first discussed on the IDEAS mailing list. It was developed through discussions with Padmadevi Pillay Esnault of Huawei and her IDEAS team.

11. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

Author's Address

Robert Moskowitz
Huawei
Oak Park, MI 48237

Email: rgm@labs.htt-consult.com