RFC7985: Security Threats to Simplified Multicast Forwarding (SMF)

Jiazi Yi, Thomas Heide Clausen, Ulrich Herberg

Internet Engineering Task Force (IETF)
Request for Comments: 7985
Updates: 7186
Category: Informational
ISSN: 2070-1721
November 2016

J. Yi
T. Clausen
Ecole Polytechnique
U. Herberg

Security Threats to Simplified Multicast Forwarding (SMF)

Abstract

This document analyzes security threats to Simplified Multicast Forwarding (SMF), including vulnerabilities of duplicate packet detection and relay set selection mechanisms. This document is not intended to propose solutions to the threats described.

In addition, this document updates RFC 7186 regarding threats to the relay set selection mechanisms using the Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP) (RFC 6130).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document analyzes security threats to Simplified Multicast Forwarding (SMF) [RFC6621]. SMF aims at providing basic Internet Protocol (IP) multicast forwarding in a way that is suitable for wireless mesh and Mobile Ad Hoc Networks (MANET). SMF consists of two major functional components: duplicate packet detection (DPD) and relay set selection (RSS).

SMF is typically used in decentralized wireless environments and is potentially exposed to various attacks and misconfigurations. In a wireless environment, some of these attacks and misconfigurations represent threats of particular significance as compared to what they would do in wired networks. [RFC6621] briefly discusses several of these, but does not define any explicit security measures for protecting the integrity of the protocol.

This document is based on the assumption that no additional security mechanism, such as IPsec, is used in the IP layer, as not all MANET deployments may be able to support deployment of such common IP protection mechanisms (e.g., because MANET routers may have limited resources for supporting the IPsec stack). It also assumes that there is no lower-layer protection. The document analyzes possible attacks on, and misconfigurations of, SMF and outlines the consequences of such attacks/misconfigurations to the state maintained by SMF in each router.

In the Security Considerations section of [RFC6621], denial-of-service-attack scenarios are briefly discussed. This document further analyzes and describes the potential vulnerabilities of, and attack vectors for, SMF. While completeness in such analysis is always a goal, no claims of being complete are made. The goal of this document is to be helpful when deploying SMF in a network and for understanding the risks incurred, as well as for providing a reference to and documented experience with SMF as input for possible future developments of SMF.

This document is not intended to propose solutions to the threats described. [RFC7182] provides a framework that can be used with SMF, and depending on how it is used, may offer some degree of protection against the threats related to identity spoofing described in this document.

This document also updates [RFC7186], specifically with respect to threats to relay set selection (RSS) mechanisms that are using MANET NHDP [RFC6130].

2. Terminology

This document uses the terminology and notation defined in [RFC5444], [RFC6130], [RFC6621], and [RFC4949].

Additionally, this document introduces the following terminology:

SMF router: A MANET router, running SMF as specified in [RFC6621].

Attacker: A device that is present in the network and intentionally seeks to compromise the information bases in SMF routers. It may generate syntactically correct SMF control messages.

Legitimate SMF router: An SMF router that is correctly configured and not compromised by an attacker.

3. SMF Threat Overview

An SMF router requires an external dynamic neighborhood discovery mechanism in order to maintain suitable topological information describing its immediate neighborhood, and thereby allowing it to select reduced relay sets for forwarding multicast data traffic. Such an external dynamic neighborhood discovery mechanism may be provided by lower-layer interface information, by a concurrently operating MANET routing protocol that already maintains such information (e.g., [RFC7181]) or by explicitly using the MANET Neighborhood Discovery Protocol (NHDP) [RFC6130]. If NHDP is used for both 1-hop and 2-hop neighborhood discovery by SMF, SMF implicitly inherits the vulnerabilities of NHDP discussed in [RFC7186]. As SMF relies on NHDP to assist in network-layer 2-hop neighborhood discovery (no matter if other lower-layer mechanisms are used for 1-hop neighborhood discovery), this document assumes that NHDP is used in SMF. The threats that are NHDP specific are indicated explicitly.

Based on neighborhood discovery mechanisms, [RFC6621] specifies two principal functional components: duplicate packet detection (DPD) and relay set selection (RSS).

DPD is required by SMF in order to be able to detect duplicate packets and eliminate their redundant forwarding. An attacker has two ways in which to harm the DPD mechanisms. Specifically, it can:

- "deactivate" DPD, making it such that duplicate packets are not correctly detected. As a consequence, they are (redundantly) transmitted, which increases the load on the network, drains the batteries of the routers involved, etc.

- "pre-activate" DPD, making DPD detect a later arriving (valid) packet as being a duplicate and will, therefore, not be forwarded.

Attacks on DPD can be achieved by replaying existing packets, wrangling sequence numbers, manipulating hash values, etc.; these are detailed in Section 4.

RSS produces a reduced relay set for forwarding multicast data packets across a MANET. For use in SMF, [RFC6621] specifies several relay set algorithms including E-CDS (Essential Connected Dominating Set) [RFC5614], S-MPR (Source-Based Multipoint Relay, as known from [RFC3626] and [RFC7181]), and MPR-CDS (Multipoint Relay Connected Dominating Set) [MPR-CDS]. An attacker can disrupt the RSS algorithm, and thereby the SMF operation, by degrading it to classical flooding or by "masking" certain parts of the network from the multicasting domain. Attacks on RSS algorithms are detailed in Section 5.

Other than the attacks on DPD and RSS, a common vulnerability of MANETs is "jamming", i.e., a device generates massive amounts of interfering radio transmissions, which will prevent legitimate traffic (e.g., control traffic as well as data traffic) on part of a network. The attacks on DPD and RSS can be further enhanced by jamming.

4. Threats to Duplicate Packet Detection

Duplicate packet detection (DPD) is required for packet dissemination in MANETs because: (1) packets may be retransmitted via the same physical interface as the one over which they were received, and (2) a router may receive multiple copies of the same packet (on the same or on different interfaces) from different neighbors. DPD is thus used to check whether or not an incoming packet has been previously received.

DPD is achieved by maintaining a record of recently processed multicast packets, and comparing later received multicast packets herewith. A duplicate packet detected is silently dropped and is not inserted into the forwarding path of that router, nor is it delivered to an application. DPD, as proposed by SMF, supports both IPv4 and IPv6 and suggests two duplicate packet detection mechanisms for each: 1) IP packet header content identification-based DPD (I-DPD), in combination with flow state, to estimate temporal uniqueness of a packet, and 2) hash-based DPD (H-DPD), employing hashing of selected IP packet header fields and payload for the same effect.

In the Security Considerations section of [RFC6621], a selection of threats to DPD are briefly introduced. This section expands on that discussion and describes how to effectively launch the attacks on DPD -- for example, by way of manipulating jitter and/or the Hash-Assistant Value. In the remainder of this section, common threats to packet detection mechanisms are discussed first; then, the threats to I-DPD and H-DPD are introduced separately. The threats described in this section are applicable to general SMF implementations, regardless of whether NHDP is used.

4.1. Attack on the Hop Limit Field

One immediate Denial-of-Service (DoS) attack is based on manipulating the Time-to-Live (TTL, for IPv4) or Hop Limit (for IPv6) field. As routers only forward packets with TTL > 1, an attacker can forward an otherwise valid packet while drastically reducing the TTL hereof. This will inhibit recipient routers from later forwarding the same multicast packet, even if received with a different TTL -- essentially, an attacker can thus instruct its neighbors to block the forwarding of valid multicast packets.

For example, in Figure 1, router A forwards a multicast packet with a TTL of 64 to the network. A, B, and C are legitimate SMF routers, and X is an attacker. In a wireless environment, jitter is commonly used to avoid systematic collisions in Media Access Control (MAC) protocols [RFC5148]. An attacker can thus increase the probability that its invalid packets arrive first by retransmitting them without applying jitter. In this example, router X forwards the packet without applying jitter and reduces the TTL to 1. Router C thus records the duplicate detection value (hash value for H-DPD or the header content of the packets for I-DPD) but does not forward the packet (due to TTL == 1). When a second copy of the same packet, with a non-maliciously manipulated TTL value (63 in this case), arrives from router B, it will be discarded as a duplicate packet.

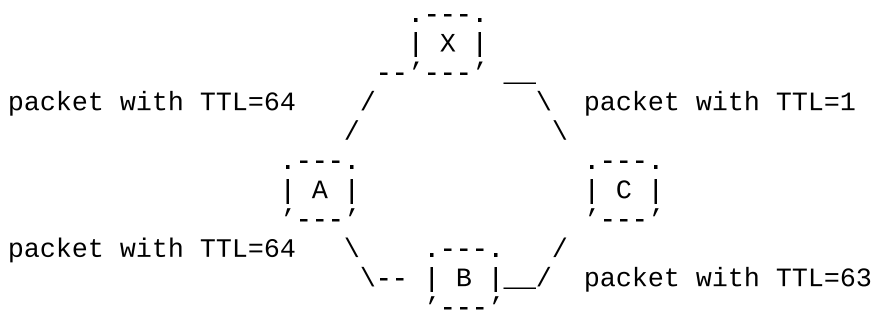

Figure 1

As the TTL of a packet is intended to be manipulated by intermediaries forwarding it, classic methods such as integrity check values (e.g., digital signatures) are typically calculated by setting TTL fields to some predetermined value (e.g., 0) -- for example, the case for IPsec Authentication Headers -- rendering such an attack more difficult to both detect and counter.

If the attacker has access to a "wormhole" through the network (a directional antenna, a tunnel to a collaborator, or a wired connection, allowing it to bridge parts of a network otherwise distant), it can make sure that the packets with such an artificially reduced TTL arrive before their unmodified counterparts.

4.2. Threats to Identification-Based Duplicate Packet Detection

I-DPD uses a specific DPD identifier in the packet header to identify a packet. By default, such packet identification is not provided by the IP packet header (for both IPv4 and IPv6). Therefore, additional identification headers, such as the fragment header, a hop-by-hop header option, or IPsec sequencing, must be employed in order to support I-DPD. The uniqueness of a packet can then be identified by the source IP address of the packet originator and the sequence number (from the fragment header, hop-by-hop header option, or IPsec). By doing so, each intermediate router can keep a record of recently received packets and determine whether or not the incoming packet has been received.

4.2.1. Pre-Activation Attacks (Pre-Play)

In a wireless environment, or across any other shared channel, an attacker can perceive the identification tuple (source IP address, sequence number) of a packet. It is possible to generate a packet with the same (source IP address, sequence number) pair with invalid content. If the sequence number progression is predictable, then it is trivial to generate and inject invalid packets with "future" identification information into the network. If these invalid packets arrive before the legitimate packets that they are spoofing, the latter will be treated as a duplicate and will be discarded. This can prevent multicast packets from reaching parts of the network.

Figure 2 gives an example of a pre-activation attack. A, B, and C are legitimate SMF routers, and X is the attacker. The line between the routers presents the packet forwarding. Router A is the source and originates a multicast packet with sequence number n. When router X receives the packet, it generates an invalid packet with the source address of A and sequence number n. If the invalid packet arrives at router C before the forwarding of router B, the valid packet will be dropped by C as a duplicate packet. An attacker can manipulate jitter to make sure that the invalid packets arrive first. Router X can even generate packets with future sequence numbers (if they are predictable), so that the future legitimate packets with the same sequence numbers will be dropped as duplicate ones.

```
                                 .---.
                                 | X |
                               --'---' __
        packet with seq=n     /          \  invalid packet with seq=n
                             /            \
                         .---.             .---.
                         | A |             | C |
                         '---'             '---'
        packet with seq=n    \    .---.   /
                              \-- | B |__/  valid packet with seq=n
                                  '---'
```

Figure 2

As SMF does not currently have any timestamp mechanisms to protect data packets, there is no viable way to detect such pre-play attacks by way of timestamps. Especially, if the attack is based on manipulation of jitter, the validation of the timestamp would not be helpful because the timing is still valid (but, much less valuable).

4.2.2. De-activation Attacks (Sequence Number Wrangling)

An attacker can also seek to de-activate DPD by modifying the sequence number in packets that it forwards. Thus, routers will not be able to detect an actual duplicate packet as a duplicate -- rather, they will treat them as new packets, i.e., process and forward them. This is similar to DoS attacks, as each packet that is considered unique will be multicasted: for a network with n routers, there will be n-1 retransmissions. This can easily cause the "broadcast storm" problem discussed in [MOBICOM99]. The consequence of this attack is an increased channel load, the origin of which appears to be a router other than the attacker.

Given the topology shown in Figure 2, on receiving a packet with seq=n, the attacker X can forward the packet with a modified sequence number n+i. This has two consequences: firstly, router C will not be able to detect that the packet forwarded by X is a duplicate packet; secondly, the consequent packet with seq=n+i generated by router A will probably be treated as a duplicate packet and will be dropped by router C.

4.3. Threats to Hash-Based Duplicate Packet Detection

When explicit sequence numbers in packet headers is undesired, hash-based DPD can be used. A hash of the non-mutable fields in the header of the data payload can be generated and recorded at the intermediate routers. A packet can thus be uniquely identified by the source IP address of the packet and its hash-value.

The hash algorithm used by SMF is being applied only to provide a reduced probability of collision and is not being used for cryptographic or authentication purposes. Consequently, a digest collision is still possible. In case the source router or gateway identifies that it has recently generated or injected a packet with the same hash-value, it inserts a "Hash-Assist Value (HAV)" IPv6 header option into the packet, such that also calculating the hash over this HAV will render the resulting value unique.

4.3.1. Attack on the Hash-Assistant Value

The HAV header is helpful when a digest collision happens. However, it also introduces a potential vulnerability. As the HAV option is only added when the source or the ingress SMF router detects that the incoming packet has digest collision with previously generated packets, it can actually be regarded as a "flag" of potential digest collision. An attacker can discover the HAV header and be able to conclude that a hash collision is possible if the HAV header is removed. By doing so, the modified packet received by other SMF routers will be treated as duplicate packets and will be dropped because they have the same hash value as previously received packets.

In the example shown in Figure 3, routers A and B are legitimate SMF routers; X is an attacker. Router A generates two packets, P1 and P2, with the same hash value h(P1)=h(P2)=x. Based on the SMF specification, a HAV is added to the latter packet P2, so that h(P2+HAV)=x’ avoids digest collision. When the attacker X detects the HAV of P2, it is able to conclude that a collision is possible by removing the HAV header. By doing so, packet P2 will be treated as a duplicate packet by router B and will be dropped.

```
              P2            P1                P2         P1
   .---.  h(P2+HAV)=x’    h(P1)=x    .---.  h(P2)=x     h(P1)=x    .---.
   | A |---------------------------> | X | ----------------------> | B |
   ‘---’                             ‘---’                         ‘---’
```

Figure 3

5. Threats to Relay Set Selection

A framework for an RSS mechanism, rather than a specific RSS algorithm, is provided by SMF. Relay Set Selection is normally achieved by distributed algorithms that can dynamically generate a topological Connected Dominating Set based on 1-hop and 2-hop neighborhood information. In this section, common threats to the RSS framework are first discussed. Then specific threats to the three algorithms (Essential Connection Dominating Set (E-CDS), Source-Based Multipoint Relay (S-MPR), and Multipoint Relay Connected Dominating Set (MPR-CDS)) explicitly enumerated by [RFC6621] are analyzed. As the relay set selection is based on 1-hop and 2-hop neighborhood information, which rely on NHDP, the threats described in this section are NHDP specific.

5.1. Common Threats to Relay Set Selection

Non-algorithm-specific threats to RSS algorithms, including DoS attacks, eavesdropping, message timing attacks, and broadcast storm, are discussed in [RFC7186].

5.2. Threats to the E-CDS Algorithm

The "Essential Connected Dominating Set" (E-CDS) algorithm [RFC5614] forms a single CDS mesh for an SMF operating region. This algorithm requires 2-hop neighborhood information (the identity of the neighbors, the link to the neighbors, and the neighbors' priority information), as collected through NHDP or another process.

An SMF router will select itself as a relay, if:

- The SMF router has a higher priority than all of its symmetric neighbors, or

- A path from the neighbor with the largest priority to any other neighbor via neighbors with greater priority than the current router does not exist.

An attacker can disrupt the E-CDS algorithm by link spoofing or identity spoofing.

5.2.1. Link Spoofing

Link spoofing implies that an attacker advertises non-existing links to another router (which may or may not be present in the network).

An attacker can declare itself to have high route priority and spoof the links to as many legitimate SMF routers as possible to declare high connectivity. By doing so, it can prevent legitimate SMF routers from selecting themselves as relays. As the "super" relay in the network, the attacker can manipulate the traffic it relays.

5.2.2. Identity Spoofing

Identity spoofing implies that an attacker determines and makes use of the identity of other legitimate routers, without being authorized to do so. The identity of other routers can be obtained by eavesdropping the control messages or the source/destination address from datagrams. The attacker can then generate control or datagram traffic by pretending to be a legitimate router.

Because E-CDS self-selection is based on the router priority value, an attacker can spoof the identity of other legitimate routers and declare a different router priority value. If it declares that a spoofed router has a higher priority, it can prevent other routers from selecting themselves as relays. On the other hand, if the attacker declares that a spoofed router has a lower priority, it can force other routers to select themselves as relays to degrade the multicast forwarding to classical flooding.

5.3. Threats to S-MPR Algorithm

The S-MPR set selection algorithm enables individual routers, using 2-hop topology information, to select relays from among their set of neighboring routers. MPRs are selected by each router such that a message generated by it, and relayed only by its MPRs, will reach all of its 2-hop neighbors.

An SMF router forwards a multicast packet if and only if:

- the packet has not been received before, and

- the neighbor from which the packet was received has selected the router as MPR.

Because MPR calculation is based on the willingness declared by the SMF routers and the connectivity of the routers, it can be disrupted by both link spoofing and identity spoofing. These threats and their impacts have been illustrated in Section 5.1 of [RFC7186].

5.4. Threats to the MPR-CDS Algorithm

MPR-CDS is a derivative from S-MPR. The main difference between S-MPR and MPR-CDS is that while S-MPR forms a different broadcast tree for each source in the network, MPR-CDS forms a unique broadcast tree for all sources in the network.

As MPR-CDS combines E-CDS and S-MPR and the simple combination of the two algorithms does not address the weaknesses; the vulnerabilities of E-CDS and S-MPR that are discussed in Sections 5.2 and 5.3 apply to MPR-CDS also.

6. Security Considerations

This document does not specify a protocol or a procedure. The whole document, however, reflects on security considerations for SMF regarding packet dissemination in MANETs. Possible attacks to the two main functional components of SMF, duplicate packet detection, and relay set selection are analyzed and documented.

Although neither [RFC6621] nor this document propose mechanisms to secure the SMF protocol, there are several possibilities to secure the protocol in the future and drive new work by suggesting which threats discussed in the previous sections could be addressed.

For the I-DPD mechanism, employing randomized packet sequence numbers can avoid some pre-activation attacks based on sequence number prediction. If predicable sequence numbers have to be used, applying timestamps can mitigate pre-activation attacks.

For the H-DPD mechanism, applying cryptographically strong hashes can make the digest collisions effectively impossible, and it can avoid the use of a HAV.

[RFC7182] specifies a framework for representing cryptographic Integrity Check Values (ICVs) and timestamps in MANETs. Based on [RFC7182], [RFC7183] specifies integrity and replay protection for NHDP using shared keys as a mandatory-to-implement security mechanism. If SMF is using NHDP as the neighborhood discovery protocol, implementing [RFC7183] remains advisable so as to enable integrity protection for NHDP control messages. This can help mitigate threats related to identity spoofing through the exchange of HELLO messages and provide some general protection against identity spoofing by admitting only trusted routers to the network using ICVs in HELLO messages.

Using ICVs does not, of course, address the problem of attackers able to also generate valid ICVs. Detection and exclusion of such attackers is, in general, a challenge that is not unrelated to how [RFC7182] is used. If, for example, it is used with a shared key (as per [RFC7183]), excluding single attackers generally is not aided by the use of ICVs. However, if routers have sufficient capabilities to support the use of asymmetric keys (as per [RFC7859]), part of addressing this challenge becomes one of providing key revocation in a way that does not in itself introduce additional vulnerabilities.

As [RFC7183] does not protect the integrity of the multicast user datagram, and as no mechanism is specified by SMF for doing so, duplicate packet detection remains vulnerable to the threats introduced in Section 4.

If pre-activation/de-activation attacks and attacks on the HAV of the multicast datagrams are to be mitigated, a datagram-level integrity protection mechanism is desired, by taking consideration of the identity field or HAV. However, this would not be helpful for the attacks on the TTL (or Hop Limit for IPv6) field, because the mutable fields are generally not considered when ICV is calculated.

7. References

7.1. Normative References

[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, DOI 10.17487/RFC6130, April 2011, <http://www.rfc-editor.org/info/rfc6130>.

[RFC6621] Macker, J., Ed., "Simplified Multicast Forwarding", RFC 6621, DOI 10.17487/RFC6621, May 2012, <http://www.rfc-editor.org/info/rfc6621>.

[RFC7186] Yi, J., Herberg, U., and T. Clausen, "Security Threats for the Neighborhood Discovery Protocol (NHDP)", RFC 7186, DOI 10.17487/RFC7186, April 2014, <http://www.rfc-editor.org/info/rfc7186>.

7.2. Informative References

[MOBICOM99] Ni, S., Tseng, Y., Chen, Y., and J. Sheu, "The broadcast storm problem in a mobile ad hoc network", MobiCom ’99 Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, DOI 10.1145/313451.313525, 1999.

[MPR-CDS] Adjih, C., Jacquet, P., and L. Viennot, "Computing Connected Dominating Sets with Multipoint Relays", Journal of Ad Hoc and Sensor Wireless Networks 2002, January 2002.

[RFC3626] Clausen, T., Ed. and P. Jacquet, Ed., "Optimized Link State Routing Protocol (OLSR)", RFC 3626, DOI 10.17487/RFC3626, October 2003, <http://www.rfc-editor.org/info/rfc3626>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

[RFC5148] Clausen, T., Dearlove, C., and B. Adamson, "Jitter Considerations in Mobile Ad Hoc Networks (MANETs)", RFC 5148, DOI 10.17487/RFC5148, February 2008, <http://www.rfc-editor.org/info/rfc5148>.

[RFC5444] Clausen, T., Dearlove, C., Dean, J., and C. Adjih, "Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format", RFC 5444, DOI 10.17487/RFC5444, February 2009, <http://www.rfc-editor.org/info/rfc5444>.

[RFC5614] Ogier, R. and P. Spagnolo, "Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding", RFC 5614, DOI 10.17487/RFC5614, August 2009, <http://www.rfc-editor.org/info/rfc5614>.

[RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, DOI 10.17487/RFC7181, April 2014, <http://www.rfc-editor.org/info/rfc7181>.

[RFC7182] Herberg, U., Clausen, T., and C. Dearlove, "Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs)", RFC 7182, DOI 10.17487/RFC7182, April 2014, <http://www.rfc-editor.org/info/rfc7182>.

[RFC7183] Herberg, U., Dearlove, C., and T. Clausen, "Integrity Protection for the Neighborhood Discovery Protocol (NHDP) and Optimized Link State Routing Protocol Version 2 (OLSRv2)", RFC 7183, DOI 10.17487/RFC7183, April 2014, <http://www.rfc-editor.org/info/rfc7183>.

[RFC7859] Dearlove, C., "Identity-Based Signatures for Mobile Ad Hoc Network (MANET) Routing Protocols", RFC 7859, DOI 10.17487/RFC7859, May 2016, <http://www.rfc-editor.org/info/rfc7859>.

Acknowledgments

The authors would like to thank Christopher Dearlove (BAE Systems ATC) who provided detailed review and valuable comments.

Authors’ Addresses

Jiazi Yi
Ecole Polytechnique
91128 Palaiseau Cedex
France

Phone: +33 1 77 57 80 85
Email: jiazi@jiaziyi.com
URI: http://www.jiaziyi.com/

Thomas Heide Clausen
Ecole Polytechnique
91128 Palaiseau Cedex
France

Phone: +33 6 6058 9349
Email: T.Clausen@computer.org
URI: http://www.thomasclausen.org/

Ulrich Herberg

Email: ulrich@herberg.name
URI: http://www.herberg.name/