presents:

IPv6 プロトコルスイートへの攻撃

ファン・ホイザー、**THC**

vh@thc.org

http://www.thc.org

目次

1. 迅速かつ短期間な **IPv6** の導入
2. 新しい **THC IPV6** アタックスイート
3. **IPv4<>IPv6** のセキュリティに該当する変更および **IPv6** におけるセキュリティの脆弱性
4. **IPv6** の実装における当面の脆弱性
5. 新しいリサーチと今後

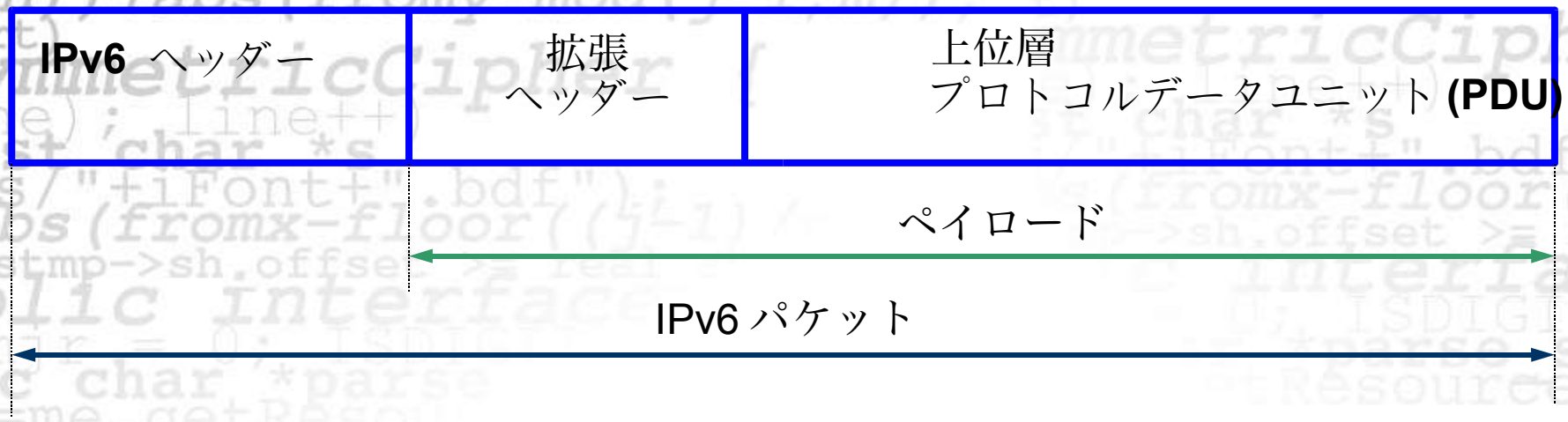
迅速かつ短期間な *IPv6* の導入

- IPv6 のゴール:
  - 次世代までも十分な IP アドレス
    - 2^{128}=340.282.366.920.938.463.463.374.607.431.768.211.456
  - IP アドレスやネットワークの自動構成
  - 階層的なアドレス構造
    - 運用コストの削減
  - セキュリティ機能の統合

IPv6 ヘッダー構造


0
4
12
16
24
31
バージョン
6
クラス
フローラベル
ペイロード長
次ヘッダー
ホップ制限
128 ビット 始点アドレス
128 ビット 終点アドレス

IPv6 層構造



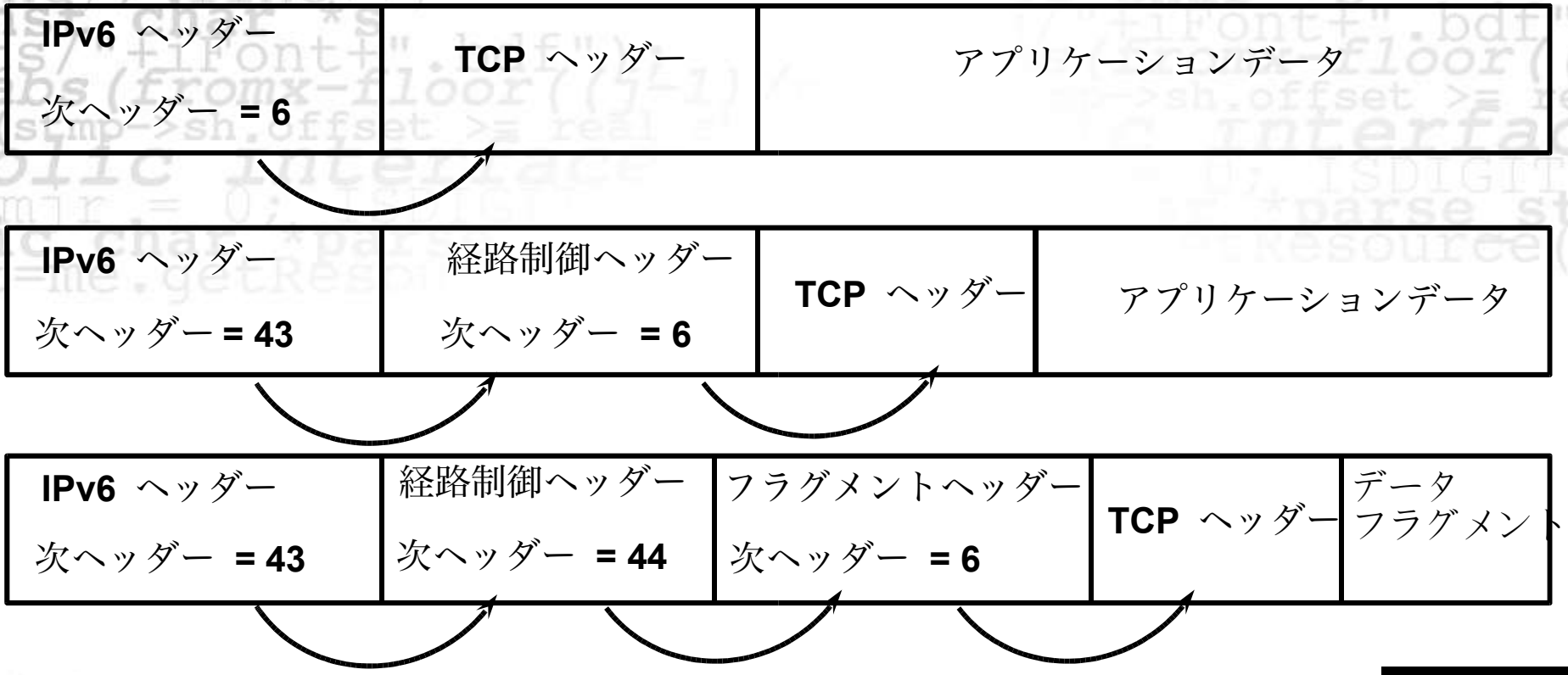
IPv6 ヘッダー　　**40** バイト

上位層 PDU　　65535 バイト

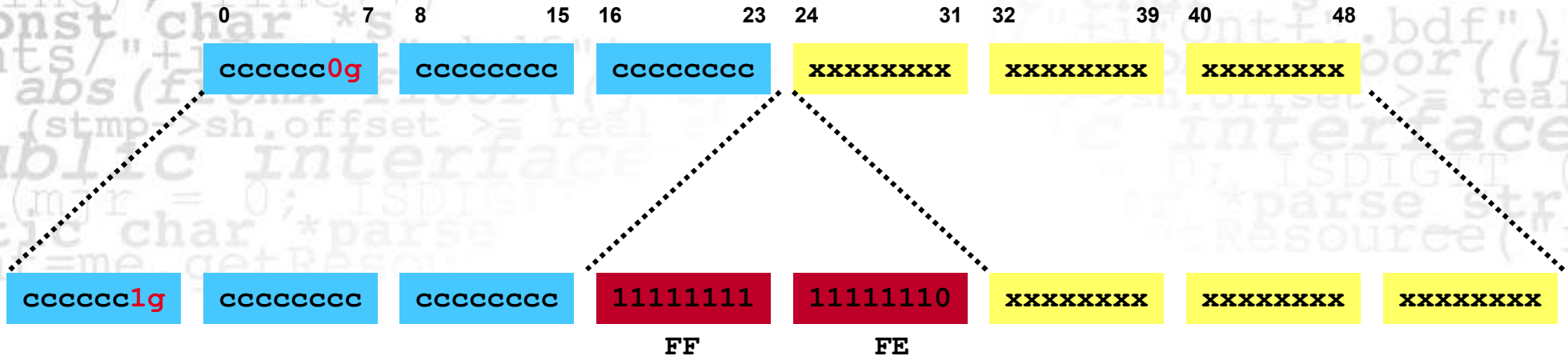
上位層 PDU　　65535 バイト = ジャンボペイロード

IPv6 ヘッダー構造

拡張ヘッダーの例： ホップバイホップ = **0**; UDP = **17**; カプセル化ヘッダー = **41**; RSVP = **46**;
IPSEC (カプセル化セキュリティペイロード = **50**; 認証ヘッダー = **51**;)
ICMPv6 = **58**; 次ヘッダーなし = **59**; 終点オプション = **60**; OSPFv3 = **98**



IPv6 インターフェイス識別子 *(EUI-64* 形式*)* マッピング

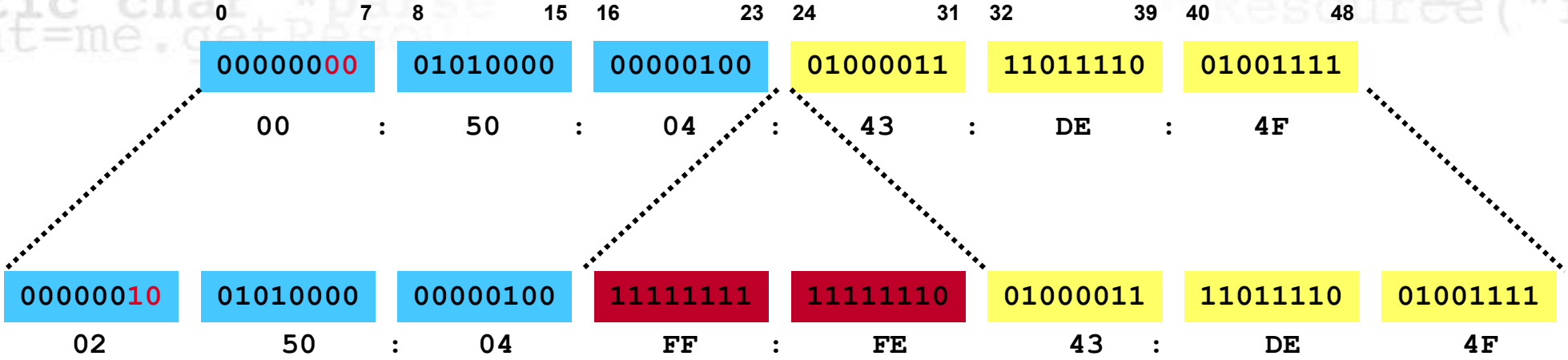


IPv6 インターフェイス識別子（ **EUI-64** 形式）
EUI: Extended Unique Identifier

c = 企業 **id**
x = 拡張識別子
g = 個別 **/** グループ **(G): 0 -** ユニキャスト　**1 -** マルチキャスト

例

```
# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:04:43:DE:4F
          inet addr:10.2.1.1  Bcast:10.2.1.255  Mask:255.255.255.0
          inet6 addr: 3ffe:ffff:100:f101:250:4ff:fe43:de4f/64 Scope:Global
          inet6 addr: fe80::250:4ff:fe43:de4f/64 Scope:Link
          ...
```



今日のブラックハットによる *IPv6* の使用

バックドアの展開

- IPv6 (6to4) の有効化
- IPv6 上でのバックドアの実行
- ポートスキャンでは発見できない
- バックドアトラフィックが検出された場合、分析が困難

InterCommunication

- Warez Exchange 、 IRC 、 バウンス攻撃に対して IPv6 InterCommunication (6to4 経由) を設定

現在利用可能なハッカーツール…

以下のハッカーツールが存在

- ポートスキャン : nmap 、 halfscan6…
- ポートバウンス : relay6 、 6tunnel 、 nt6tunnel 、 asybo…
- サービス妨害 (DoS 、接続のフラッディング): 6tunneldos
- Packet Fun: isic6, libnet (部分的な実装のみ)

IPv6 を特に狙った攻撃ツールは今のところ存在せず

IPv6 の開発が広がればこの状況の変化は必至

… しかし、それを待っていたくはありませんね？

THC IPV6 アタックスイート

- THC は使いやすい IPv6 パケットファクトリライブラリを開発
- 多くの IPv6 プロトコルエクスプロイトツールがわずか 5 ～ 10 行でコード化可能
- 多くの強力なプロトコルエクスプロイトを既に網羅

- 現在のコードの警告
  - Linux のみ
  - Little Endian
  - 32 ビット
  - イーサネット

THC IPV6 アタックスイート

- 実装は簡単！
- Redirector redir6.c の始点の 90% に 2 つのスライド
- ICMP6 エコー要求の送信
  - pkt = thc_create_ipv6(interface, PREFER_GLOBAL, &pkt_len, *src6*, ***target6***, 0, 0, 0, 0, 0);
  - thc_add_icmp6(pkt, &pkt_len, ICMP6_PINGREQUEST, 0, 0xdeadbeef, NULL, 0, 0);
  - thc_generate_and_send_pkt(interface, NULL, NULL, pkt, &pkt_len);
- Target6 は ICMP6 エコー応答で返信

THC IPV6 アタックスイート

- Ping の後に ICMP6 Redirect を送信
  - ipv6 = (thc_ipv6_hdr *) pkt;
  - thc_inverse_packet(ipv6->pkt + 14, ipv6->pkt_len - 14);
    - この機能はエコー要求パケット をエコー応答パケットに転換
  - thc_redir6(interface, *oldrouter6*, fakemac, NULL, ***newrouter6***, mac6, ipv6->pkt + 14, ipv6->pkt_len - 14);
    - この機能は ICMP Redirect を送信し、*src6* に古いデフォルトルーターである *oldrouter6* でなく ***newrouter6*** を埋め込む
- これでトラフィックは newrouter に送信されるようになります。

THC IPV6 アタックスイート - ツール

- PARSITE6
  - 中間者攻撃用 ICMP 近隣スプーファ
- DOS-NEW-IPV6
  - LAN (DAD スプーフィング) 上のすべての新しい IPv6 システムアクセスを拒否
- REDIR6
  - トラフィックを LAN 上のシステムへ向け直す
- FAKE_ROUTER
  - ルーターになりすまし、ルートを埋め込み、デフォルトのルーターになる…
- SMURF6
  - ローカルスマーフツール (自分の LAN を攻撃)
- RSMURF6
  - リモートスマーフツール (リモート LAN を攻撃)

THC IPV6 アタックスイート - ツール

- TOOBIG6
  - ターゲットの MTU を減少させる
- Alive6-Local
  - すべてのローカル IPv6 システムを検索する
- Alive6-Remote
  - リモート LAN のアライブ IP6 システムを検索する
- プロトコル実装テスター
  - 断片化 + 経路制御ヘッダー
  - マスヘッダー
  - 無効なポインタ
  - …

>> このプレゼンテーションまで：新しいツール <<

IPv4 から *IPv6* へのセキュリティに該当する変更

- 要旨:
  - IPv6 と IPv4 のセキュリティはよく似ている
  - 基本的なメカニズムは同じ
  - アプリケーション 層は影響なし
  - IPv6 には IPSec が含まれているが現在使用されていない
  - IPSec はインターネットアプリケーションのアプリケー ションレベルへの攻撃は阻止しない

セキュリティに該当する変更の概要

1. プロトコルの変更
2. 偵察
3. ローカルアタック : ARP 、 DHCP
4. スマーフ (トラフィック増幅)
5. 経路制御 & 断片化攻撃
6. IPv4 と IPv6 の共存

1. プロトコルの変更

- ほとんどの IP ヘッダーのコンテンツおよびオプションは 削除されていない
  - IP ID フィールドなし
    - 稼働時間のチェックができなくなった
  - IP レコードルートオプションなし
    - 代替の経路探索がなくなった
- ブロードキャストアドレスは存在しない
- マルチキャストアドレスはリモートから終点を指定できない
  - アライブスキャンに重大な問題!

2. 偵察 *IPv4*

サブネットのネットワークサイズは通常 **2^8 = 256**

通常の攻撃方法

1. Ping がターゲットリモートクラス C にスウィープ (5 ～ 30 秒で可能)
2. ポートがアライブホストをスキャン
3. 有効なポートの脆弱性テスト

さまざまなツールが利用可能

- Nmap
- Amap
- Nessus
- ...

2. 偵察 *IPv6 (1/2)*

サブネットでネットワークサイズが **2^64 (** 変動あり **)** に増加

- サブネットで可能なホスト数は 18.446.744.073.709.551.616
- Ping のスウィープは膨大な時間を消費
  - 総当り : ***5*** 億年
  - 知恵 + テクノロジーの発達 : 依然数ヶ月
- パブリックサーバーはパブリック DNS にある必要あり
- 管理上、すべてのホストはプライベート DNS にある必要あり

>> DNS サーバーは主要な情報源 **<<**
>> （そして主要なターゲット）になる **! <<**

2. 偵察 *IPv6 (2/2)*

- ローカルネットワーク(ルーター、 DHCP 、時間など) 内のキーサーバーを特定するための標準化マルチキャストアドレスが新たなチャンス
- ローカルマルチキャストでは、 1 つのホストのセキュリ ティが侵害されると、その他すべてのホストがサブネットに入る
- 単一ホストのテクニックは変わらず (ポートスキャン、有効なポートへの攻撃、エクスプロイトなど)
- ネットワークのリモートアライブスキャン (Ping スキャン) は不可能になる

2. THC-IPV6 アタックツールキットによる偵察

- alive6-local – ローカル / リモートのユニキャストターゲットおよびローカルのマルチキャストアドレス用
  - 種類のパケットを送信
    - ICMP6 エコー要求
    - 知られていないヘッダーを持つ IP6 パケット
    - 知られていないホップバイホップオプションを持つ IP6 パケット
    - IP6 フラグメント (最初のフラグメント)
- alive6-remote – リモートマルチキャストアドレス
  - 上記と同じだが、すべてのパケットをターゲットネットワークのルーター用に 2 つのフラグメントと 経路制御ヘッダーで送信
  - ターゲットルーターがマルチキャストアドレスに経路制御ヘッダーエントリを認める場合のみ有効 – 問題のある実装が必要 ! (リサーチを参照)

3. DHCP IPv4

- DHCP はブロードキャストメッセージを利用
- 合法的なものでなく、Rouge デバイスが応答
- 「中間者」攻撃を実行するために、ホストに新しい DNS および経路制御情報を提供

3. ARP IPv4

- ARP はローカルネットワーク上で IP > MAC を実行するために Layer 2 ブロードキャストを使用
- 攻撃者は「中間者」攻撃を実行するために応答

3. ARP/DHCP IPv6

- 両方のプロトコルにセキュリティの追加なし
- ICMPv6 ステートレス自動構成 = DHCP light
- ICMP6 近隣探索および近隣要請 = ARP 置き換え
- NS ベースの重複アドレス検出により、要求に応答することでホストに対する DoS が可能に

3. ICMPv6 ステートレス自動構成

1. RS:
ICMP タイプ **= 133**
Src = ::
Dst = FF02::2
クエリ **= RA** を送信

***fake_router6*:**
全 **IP** をデフォルトの
ルーターとして設定

2. RA:
ICMP タイプ **= 134**
Src = ルーターリンクローカルアドレ
Dst = FF02::1
データ **=** オプション、プレフィック
、
有効期間、***autoconfig*** フラグ

- ルーターは定期および要請ルーター広告 **(RA)** を全ノードマルチキャストアドレス **FF02::1** に送信
- クライアントは経路制御テーブルやネットワークプレフィックスを広告から構成 **=> IPv4** の **DHCP-light** と同様
- ただし、ルーター広告は誰でも送信可能 **! =>** ***fake_router6***

3. ICMPv6 近隣探索

1. NS:
ICMP タイプ = 135
Src = **A**
Dst = 全ノードマルチキャストアドレス
クエリ = 誰が IP **B** を持っているか？

***parasite6*:**
各 **NS** に応答し、**LAN** 上の各システムであると主張

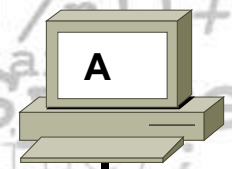
2. NA:
ICMP タイプ = 136
Src = **B**
Dst = **A**
データ = リンク層アドレス

A が **B** の **MAC** アドレスを必要とする場合、全ノードマルチキャストアドレスに **ICMP6** 近隣探索を送信

B は **A** への要求や応答を **MAC** アドレスで確認 **=> IPv4** の **ARP** と同様

ただし、誰でもこの要求に応答可能… **=> *parasite6***

3. ICMPv6 重複アドレス検出 (DAD)



1. ND

1. NS:
ICMP タイプ = 135
Src = :: (指定なし)
Dst = 全ノードマルチキャストアドレス
クエリ = 誰が IP **A** を持っているか？

***dos-new-ipv6*:**
各 **NS** に応答し、**LAN** 上の各システムであると主張

2.
誰も指定の IP アドレスを持っていない場合は応答

なし

A が新しい **IP** アドレスを設定した場合、重複アドレス検出チェック（**DAD**）を行い、そのアドレスが既に使用されていないか調べる

DAD チェックには誰でも応答可能… **=>** ***dos-new-ipv6*** は **LAN** 上の新たなシステムを阻止

4. スマーフ *IPv4*

- ブロードキャストアドレスにスプーフされたパケットを送信することで単一のターゲットに応答を送信 (例： ICMP エコー要求 / 応答)
- トラフィック増幅
- ターゲットリンクの DoS

4. スマーフ *IPv6*

- ブロードキャストアドレスなし
- さまざまなマルチキャストアドレスに置き換え
- 終点がマルチキャストアドレスである場合、 RFC 2463 は ICMP 応答が送信されないように指定。ただし、例外あり。
  - Cisco Security Research のやり方は間違い
- 攻撃可能か？
  - ローカル： 可能！
  - リモート： 経路制御ヘッダー、断片化などの実装による

4. THC-IPV6 アタックツールキットによる IPv6 のスマーフ

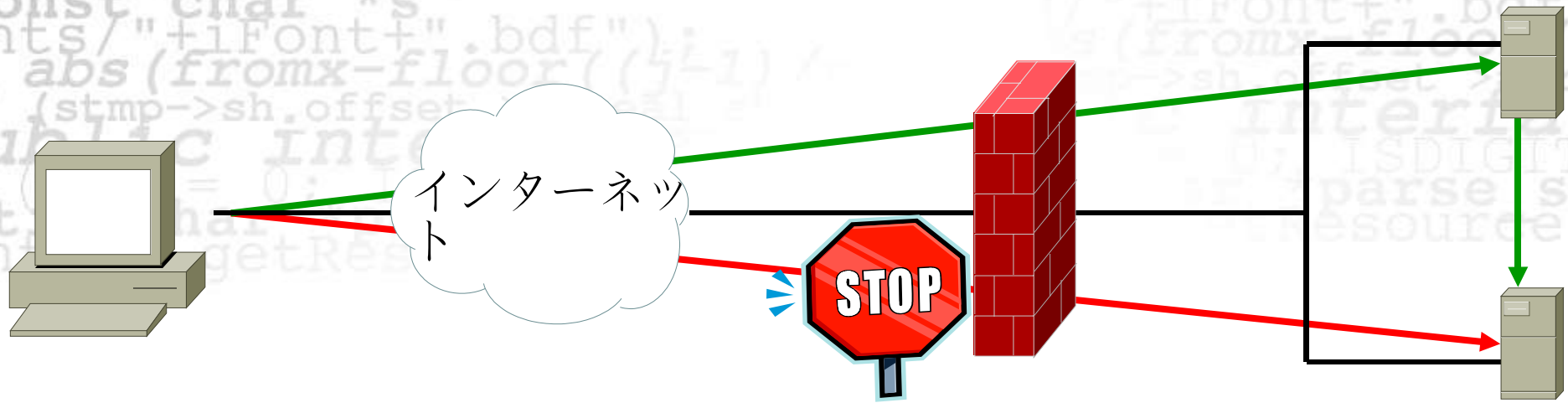
- smurf6 – ローカルで実行されるスマーフ用
  - 始点はターゲット、終点はローカルマルチキャストアドレス
  - 膨大なローカルトラフィックが生成され、始点に送信される
- rsmurf6 – リバーススマーフ、実装ミスを悪用 (例: Linux)
  - 始点は全ノードマルチキャストアドレス (*IPv6* スピークの *255.255.255.255*) 、終点はターゲット
  - ターゲットが IPv6 (例： Linux) を実装ミスした場合、全ノードマルチキャストアドレスにエコー応答で返信し、膨大なトラフィックを生成
  - ローカルの LAN で、 100 台の Linux サーバーを持つネットワークの 1 つのパケットが合計 1 万の処理済パケットを生成 !

5. 経路制御プロトコル

- ほとんどの経路制御プロトコルは独自のセキュリティメカニズムを提供
- これは IPv6 でも同じ
- セキュリティプロパティを持たず IPSEC の使用に頼る OSPFv3 は例外

5. 経路制御ヘッダーの操作

経路制御ヘッダー攻撃
(IPv4 ソースルーティングと同様 **)**

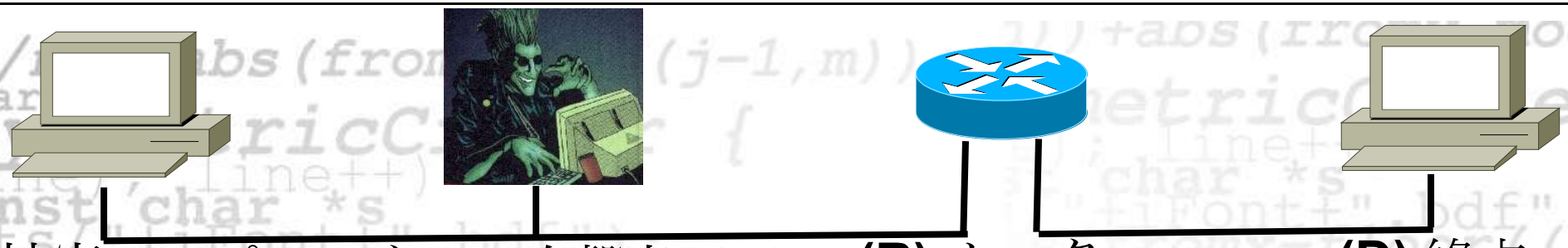


alive6-remote を使用して 経路制御ヘッダーがターゲットとなるかどうかをチェック

5. ICMP6 Redirects によるルートの埋め込み

- システムがパケット用に誤ったルーターを選択した場合、ルーターは ICMP6 Redirect パケットで送信者に報告
- 有害なシステムが悪いルートを埋め込まないようにするために、ルーターは対抗するリダイレクトパケットを送信する必要がある
- システムがターゲットに送信している、リルートしたいパケット全体を予測できれば、どのようなルートも実装可能！しかし、どのように行うか？
- 簡単 –エコー要求のふりをすれば、それに対する応答を理解可能！☺

5. ICMP6 Redirects によるルートの埋め込み



1. (A) 攻撃者がエコー要求を送信
   始点 : (D) 終点、終点 : (V) 被害コンピュータ
2. (V) 被害コンピュータがエコー要求を受信し、 (D) に応答を送信
3. (A) 攻撃者が Redirect を作成
   始点 : (R) ルーター、終点 : (V) 被害コンピュータ
   (D) への全トラフィックを (A) に向け直す

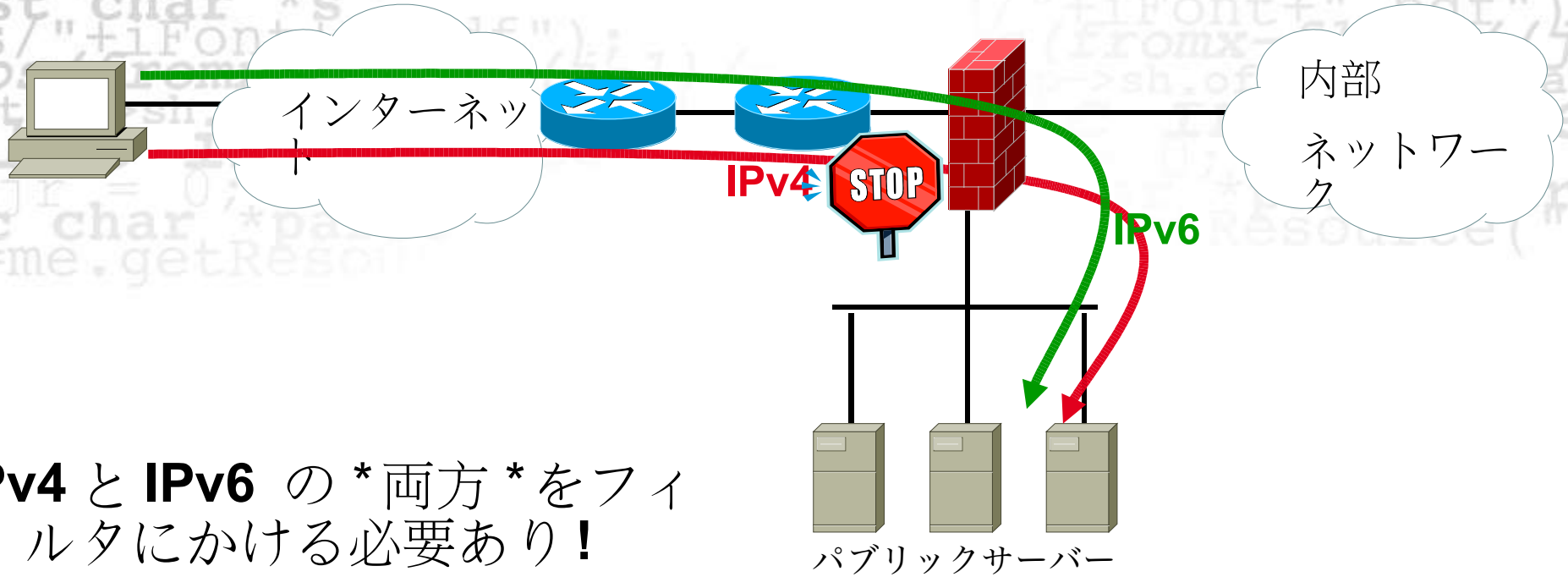
THC-IPV6 アタックツールキットで ***redir6*** が実行

toobig6 の同じコンセプトで (V) 被害コンピュータの M

5. 断片化

- 断片化はルーターでなく 始点で実行、再構築は 終点でのみ実行
- 再構築の後、断片化が最初で経路制御ヘッダーが後に来る場合、パスのルーターは経路制御ヘッダーを用いたパケットをドロップできない

6. デュアルスタック攻撃



IPv4 と **IPv6** の *両方 * をフィルタにかける必要あり!

IPv6 の実装における当面の脆弱性

- Python 03/2004 (IPv6 なしでコンパイルした場合)
  - IPv6 アドレスで DNS 応答を送信するとクラッシュ
- Ethereal 03/2004
  - 構文解析バグ、リモート攻撃可能
- Apache 09/2004
  - URI 構文解析バグ、リモートクラッシュ、 おそらく攻撃可能
- Exim (MTA) 01/2005
  - バッファオーバーフロー、ローカルの特権昇格
- Cisco IOS 01/2005
  - 複数の不正パケットを受信した場合にリモートクラッシュ
- Postfix 02/2005
  - IPv6 config file がない場合にスパムを許可
- Linux Kernel 02/2005
  - 長さ認証バグ、リモートクラッシュ、 おそらく攻撃可能

リサーチおよび実装テスト

- マルチキャストの終点にパケットの応答
- マルチキャストアドレスの始点からパケットの応答
- 経路制御ヘッダーからマルチキャストアドレスへ
- 断片化およびそれに続く経路制御ヘッダー
- マルチキャストリスナー検索のクロスボーダー経路制御 **(ttl > 1)**

THC による今後の *IPv6* セキュリティリサーチ

- Multicast Fun
  - Global Multicast FF:0E エクスプロイト
- IPv4 <> IPv6 共存ソリューション
  - トネリングにおけるセキュリティの脆弱性

IPv6 への今後の脅威や危険

1. **IPv6** を特に狙ったアタックツールの開発
   - 既存の IPv4 アタックツールと大差なし
2. ワーム
   - TCP/IP ワーム (例： Slammer タイプ) は今後消滅
   - 電子メールワームは存続
   - メッセンジャーワームおよび P2P ワームが拡散
3. **DNS** サーバーが主なターゲットになる
4. 攻撃は **LAN** の侵害されたサーバーからクライアントへの攻撃へ移行
5. **IPSEC** が広く展開された場合、 認証の盗みがセキュリティに関する主な懸念となる

IPv6 でのインターネットセキュリティに関する結論

現在のところ **IPv6** に対する新たなリスクはないものの、**IPv4** に対するセキュリティの改善点がいくつかあり

- アライブスキャンや TCP/IP ワームは非常に困難
- IP レコードルートオプションが削除されると、稼働時間のチェックがなくなる
- ネットワークフィルタや攻撃の追跡が容易に

IPSEC の導入で **IPv6** がセキュアになるわけではないが、攻撃の追跡が容易になり、スニッフィングや中間者攻撃が非常に困難に

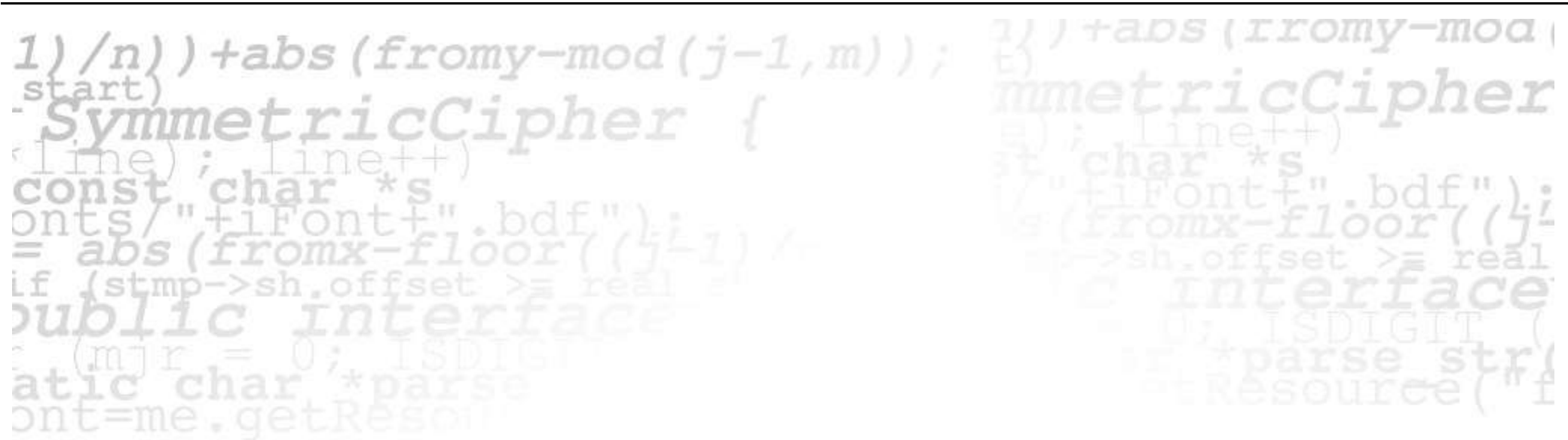
いくつかの推測は明らかではないため、リサーチが必要

質問は？

Have fun!

どうもありがとう
ございました

(ダウンロード先 : www.thc.org)


1)/n))+abs(fromy-mod(j-1,m));
start)
SymmetricCipher {
const char *s
= abs(fromx-floor((j-1)/
if (stmp->sh.offset >= real
public interface
atic char *parse