IRS (Inter-Domain Routing Security) ミーティング　議事録

日程 : 2004/07/07 七夕
場所 : シスコシステムズ（赤坂国際ビル14F)
Chair : 吉田友哉、近藤邦昭
プログラム：導入PPT参照

議事録の見方：
＋、－：発表者発表
☆、○：参加者側質問、コメント

近藤さん：
　＋議論
　　－経路自体は綿密な運用で危機回避できるが、プロトコル的なものは難しい
　　－何が出来るの？を検討しよう！

　＋論点
　　－Inter-Domain（AS-AS間)で流れるプロトコル(BGP4)に焦点
　　　AS内はAS内管理である、と前提する
　　－L2以上
　　－経路情報の信憑性、その維持について
　　－セキュリティについて

美也さん：

１．現状
　＋NANOG31開催中にCisco本社で Security Workshopを開催
　　－AT&T
　　　Receive ACLをGRP protectionに使っている
　　　Triggerd Blackholeなどもやっている
　　　その他色々やっている(資料にリストあり)

　　　Versionによらない実装が欲しい
　　　NetflowなどにConsistencyが欲しい
　　　ソフト共通の使用が欲しい

　　－Sprint
　　　MIBで色々欲しい
　　　ルータで余計なPortが空いていたりしている
　　　ACLが使い難い
　　　BGPで機能が増えるのはいいがCLIが多すぎる
　　　MaxPrefixの処理に問題あるのでは？
　　　BGPピアへ対するadvertised-routeが見たい
　　　SourceTrackerで、特別なトラフィックパターンを検出して処理を走らせて欲しい

☆MaxPrefixについてどうおもうか
　○MaxPrefix受け取ったら落としっぱなしが良いよね
　○Prefixのサイズに依存して処理を走らせるような処理にしてほしい
　○落とす、のではなくてUpdateを受け取らない
　○とにかく選びたい！
　○Capabilityに受信経路(期待)数を含めて送信させる仕様をIETFで検討している

☆AdvertisedRouteをsummaryで出して欲しい
　○Ciscoはsummary表示が無い
　○CiscoはOutband Filter後のadvertised-filterが見えない

　　－Verio
　　　設定のGlobal applyが欲しい
　　　早くアタックを止めさせる為の方法に言及
　　　・BGPで設定を伝播させるような仕組みとか。。。

　　－MCI

全てのInterfaceにLineLateでACLが動いて欲しい
・CoreRouterでも同様

＋まとめ
－Consistency！

☆どうしてVerioはマルチベンダー？
○やっぱりシングルベンダーはセキュリティ等に問題がある

２．動向
＋Control Plane
－GeneralizedTTL
－シンタックスチェック・シネマテイックスチェックがある

＋Guarded Trust
お互いに疑って、Ingress/Egress Filterを書くこと
一般的にDeployされている？
○例：ASとPrefixでand条件を付けている
○例：MaxPrefixや受け取りたくないPrefixを設定

＋MD5
Key Distributionはマニュアルしかない…？

＋BGP over IPsec
draftもある
本当に必要？

＋TTL Sanity Check
BGP TTL security hack
Generalized TTL security Mechanism
特別なTTLだけを受け取るような設定
Draftはあるが実装はもうそろそろ

＋Forwarding
UnicastRFT
Netflow

＋Management Plane
使用しないProtocolは落としましょう

３．今後
＋まずは今出来ていないことをやるべき
Ptomanine
RPsec

＋現在出来ること
ルータ事態の保護
PeeringRelationship保護
不要ルーティング情報の保護
routing flapsなど

－さらなる(違う)観点のセキュリティ
S-BGPやso-BGPなど

＋so-BGPの考え方
いかなる種類のCentral authorityには依存しない
S-BGPは非現実的では？というのがdraftの動機
一斉に適用は非現実的、選択肢も欲しい
ルーティングを保護する為にルーティングを使うのはどうなの？
Updateとセキュリティは別議論

☆so-BGPだけで独立して信憑性が取れる？

○外部証明ならIRRでも良い
○みんながIRRを見に行けばいい
○certでは14万、20万経路を暗号解読するのに負荷がかかる

４．SO-BGPのオペレーション
＋Certificate Transport
so-BGPはTransport非依存
どのようにCertificateがso-bgpルータに届くかはスコープ外

＋Certification Operation
資料参照
＜ヘルプ＞
公開鍵を作る。PGPのようにWebTrustで。
Entity-CertをAS間で交換する
各Certを交換

＋Deployment Option
サーバが代替してiBGPから情報を集めcertificate処理をオフロードできる
サーバ同士がmultihop eBGPで情報交換
ThirdParty機関を介してcertificationも可

＋Incremental Deployment
＋PathとPrefixをvalidation
eBGP multihopなどをつかってcertificationを交換する
validationはneighborで無くても可能

＋本当に必要？実装・運用に値するか？

５．最後に
よいFeedback Loopを作りましょう

☆Control，Forwarding，Management各planeが同じ土俵に載っているのが問題なのでは？

○IP-VPNなどでは分けて運用している
○物理的に分けたり論理的に分けたり
○トンネル張ったら負け
○Vlan-TAGで区別すれば論理的に分離可能
○ControlPlaneとManagementPlaneが同じだからこそ上手く働いている部分もある
BGPなどはBGP-sessionだけ張れてF.planeが落ちたらまずい
○ルータ側で実装もしている
○gMPLSなどでその発想はある
○ルーティング部分の保護の努力は続けているが、分ければ不要になる
○NextHopを書き換えて、Peerルータと転送ルータを分ける事例もある
○F.planeとC.planeが一致していないと、C.planeでF.planeの情報も伝播しなければならない
○ルーティングプロトコルの保護は自動でインプリして欲しい
インプリはされてるけどエンバグされる
○全部MPLSでつなぐと、end-endしか見えないのでセキュアになる
○IXセグメントがreachabilityである必要は無い。
○IPv6ではUnreachなセグメント。Traceは出来るがPingを打つと届かない。
○ラベルパスで網を守る方法もある

☆そもそもそこまでセキュリティは必要？
○見えざるものに対する脅威の対策
○BGPでTCP-MD5を使うほどの脅威は本当にあるのか？万全でもない。
○DNS-secの方が重要となるはず。例えば無線でfaked DHCPするのは簡単
○TCP-MD5も万全ではない。FreeBSDはone-wayでも動く。
○TTLの設定が、脅威もインプリもリーズナブル
○IXをPrivateにすると、マルチホームしてバランスを考えたりすると破綻するのでは
○Certificateを作ってまでOriginを認証する必要がある？

☆so-BGPは先に経路を受け取るの？
○経路を先に受け取ってその後認証を行う
○path認証を行おうとすると、数Hop先で破綻しそう

☆Ciscoのso-BGPの開発はCiscoの意思？
　○BGP関連の開発者がインプリしてる
　○Cisco内では自由に何でもやって、という風潮もある

☆AS-pathとPrefixはandできる？
　○今後設定をインプリできる
　○設定をたくさん書けば出来る
　○設定ファイルをBGPで送ればいける？？

吉田さん：「TCP Vulnerabilityに願いを・・・」

２．TCP Vulnerabilityアナウンス
　＋4/21にJPCERTで発表
　＋NISCCでMD5推奨の話をしていた
　　詳細やMD5で完璧かには言及されていない
　＋SNMPトラブルが同じ日に発表された。
　　こちらの方が痛い
　　あるルータではBGP用のTCPセッションに一定のPort#を使っている為、
　　それを調べられてツールで一気にアタックされると非常に痛い

３．満を持して出てきたTCPドラフト
　＋4/21にOO.txtが発表
　＋RSTやSYNに対しACKしてから落とす仕様
　＋01.txtでRST＋SYNに対するattackとinjection対策が盛り込まれた
　＋確率(WindowSize)の幅が減る、というだけで32bit全てでアタックされたら一緒

４．TCP Vulnerability 何が痛い？
　＋BGPとDNSが危ない、というのがWite Houseのペーパーにあったりする
　＋BGPは特に痛い
　　アドレスはバレバレ、BGPの片方はport179
　　セッション保持が長い
　　WindowSizeも大きい

５．Message Digest 5
　＋簡潔さ、安全性、速度を重視
　　調べつくされて、ツールで一気にアタックされると非常に痛い
　＋RFC1321
　○採用すると経路計算が遅くなる(ベンダーの仕様次第？)
　　網内で使うと影響が出てくる？
　＋TCPヘッダのオプションフィールドに突っ込まれる

６．ルータのインプリ
　＋殆どのベンダで実装済み
　＋パスワードに使用する文字に関して、マニュアルと異なる場合がある
　＋鍵交換、管理が大変
　＋PGPを使っている人はほとんどいない

☆一度設定したパスワードを見直したいけど…
　○古いJUNOSは平文で見える

７．MD5問題諸々
　＋MD5の利用を前提としていない装置がある
　　ヘッダの中身を勝手に変更⇒当然Hashも変化　など
　＋ヘッダーが増える
　　RFC2385：TCPのoptionを考慮したうえでMSSを減らして通知
　　RFC879：自分と相手で小さいMSSを選択
　　ルータ間でTCP MSSを変えてもEnd-Endには問題無し
　　でも、相手次第ではフラグメント発生、そのままBGP down...
　＋FreeBSDはTCP/MD5のOneWayサポートしている
　　BGP View開発環境はFreeBSDのため認証OneWayだった

８．IXの対応
＋各IXとして、基本はISPにお任せ
＋JPIXとしては利用者の意見を集めていて、次回ユーザ会までに答えを出したい
鍵配送、交換の問題がクリアー出来ない…TTL Hackなどベンダー対応して欲しい

対策としてもDefault Passwordしか思いつかない…
漏れたり、同じ鍵を使い続けると危険が増す。
結局鍵更新が難しいし、BGPを落とすのでコストも大きい

９．対策
＋TTL Hack
－RFC3682：the Generalized TTL Security Mechanism
＋RPF Check
ルーティングテーブルをLookupすることによりspoofを検知
実装は少ない、エッジは非力なルータなので使い難い
＋フィルタリング
－正規のBGPピア以外からのBGPパケットをフィルター
Operationで頑張るしかない、multihopなどには要注意
○アタックは一方向なので、自分は守れない
○IXセグメントにOutband Filterを書くことで相手を守ることは可能
＋アドレスをPrivate化してしまう
いろいろ問題もありやりたがらない
＋BGP No Announcement
IXのセグメントをBGPに流さない…でも、いまさら難しい。
Routableかどうかは ISP依存になってしまう

☆ループバック同士でPeer張ればよいのでは？
○TTLを管理しないと、BGP sessionが迂回される可能性がある

10．危険性
＋DNSから推測されることが多い。

☆ほんとに、ルータがMD5に影響を受ける変更をするの？
○ルータがMD5に対応していないと、MD5パケットのIPオプションを見て
ドロップしちゃう可能性がある？

☆110ISPとミラーしているが、MD5化要求があったのは1割程度だった

☆Ciscoのある実装で、RSTを一度に受けると一定間隔でしか受け付けない仕様がある
○正規のRSTが受け付けられない危険がある…でもレアケース

鎌田さん：JPCERT/CC AS ミーティング報告
１．JPCERTがTCP脆弱性対策でやったこと
＋国内ベンダーに技術情報などを通知(３月～４月)
＋Weekly Reportを作成し、TCP MD5の紹介
ねたに困ったのでねた募集中！
＋4/19にASを集めてミーティング衆知

２．アンケート実施
＋4/19に当日＆後日アンケートを実施
＋MD5の設定状況を確認
4/7, 4/19, 4/19- で意識が高まり、設定ASが増える
○MD5認証NGによってBGPアタックのログが出る

３．事前の情報提供について、JANOG14でパネルします

☆JPCERTがやったことについて
○詳細情報が無かったので、影響が見えないのはもやもやする
○ベンダーに伝わっていたのか判らない
○ライトスタッフへの情報提供は不十分であった
○詳細を伝えることは、攻撃方法を伝えることとイコールとなる
○チャレンジとしては評価できるが、不満もある
○相性問題、ベンダー対応問題まで情報が出ていると嬉しかった

　　ベンダーに情報を提供して状況を確認する、など方法があるのでは？

☆攻撃方法(ツール)が世に出ているか、などの情報は出せなかったのか
　○公開事前では攻撃ツールは未確認、事後ではキャッチしていた
　○ツール公開有無は重要度の判断となる
　○ツールがある、という情報が伝わると攻撃者も増える
　○ツール公開を周知しなかったことはJPCERT側で反省
　○公開時間は検討しないといけない
　○ツールは昔からあったが、やりやすさなど環境が変化した

西野さん：IXの保護
１．対策案
　＋全員がIngress Filterを設定すれば攻撃パケットは来ない
　＋インターネット側からIXセグメントへのパケットはフィルターしている
　＋IX利用者がOutbandフィルターを設定する…幸せになるのは相手だけ
　＋自分の顧客にフィルターをかければ自社内攻撃は防げる
　＋Non-routableは検討したけれど…
　○IX SWをL3SWにしLayer3まで見て、攻撃パケットをドロップさせればどうか？
　＋MacAddressフィルターは準備している
　　JPNAPも準備し、一部適用している
　＋xSPによっては、大きく設定変更を要する会社がいるのでは。

☆PEでのIngress Filter設定を推奨すると困るのか？
　○ソースアドレスレベルでIngress Filterを書いているか？
　　書いている例もある。挙手は数人。
　○PEでDistination Filterを書いているか？
　○IX接続ルータでブラックホールを作れば良いのでは？
　○uRPFのloose modeは意味が無いが、Strict modeはMultihome modeでは使えないのでは
　　コマンド設定で対応可能　⇒　[janog:05620]で補足説明済み

近藤さん：まとめ
　＋次回について
　　－３ヶ月に１回くらい。次回は10月くらい？
　　－発表者候補は慶樹さん
　　－uRPFセミナーが事前に欲しい

　＋経路の信頼性について
　　－IRRやso-BGPなど、手法は色々ある
　　－とにかく、コンフィグに落ちて欲しい
　　－Cisco頑張れ

　＋BGPのセッションに関するアタックについて
　　－TCP MD5が簡単ではないが一番簡単だろう。
　　－IXセグメントをUnroutableにする、Filterするなどの対策がある
　　－iBGPのケアも今後したい
　　－eBGPを保護するようなオペレーションをしたほうが良いでしょう

　＋提案etc
　　－「こういうフィルターを作ればいいんじゃないの？」
　　－絵を描いて、次回につなげましょう