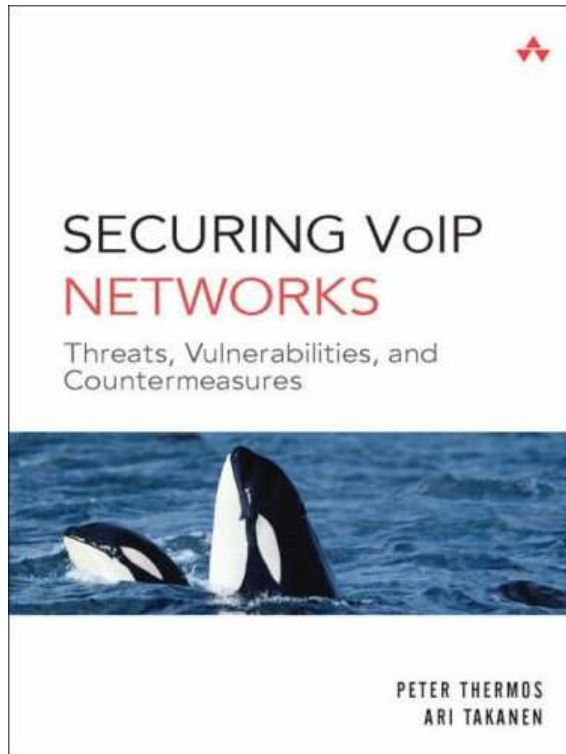


## Securing VoIP Networks: Threats, Vulnerabilities and Countermeasures

Peter Thermos,  
CTO, Palindrome  
Technologies

Ari Takanen,  
CTO, Codenomicon





## Securing VoIP Networks: Threats, Vulnerabilities and Countermeasures

Peter Thermos,  
CTO, Palindrome  
Technologies

Ari Takanen,  
CTO, Codenomicon





**NOTE:  
THIS PRESENTATION IS BASED ON THE BOOK**

The views presented here are not necessarily  
those of Codenomicon or Toyo





**注意:**  
このプレゼンテーションは、同書に基づいています

ここに述べられる見解はCodenomicon社及び東陽  
テクニカのものではありません





## Contents



- Chapter 01: Introduction
- Chapter 02: VoIP Architectures and Protocols
- Chapter 03: Threats and Attacks
- Chapter 04: VoIP Vulnerabilities
- Chapter 05: Signaling Protection Mechanisms
- Chapter 06: Media Protection Mechanisms
- Chapter 07: Key Management Mechanisms
- Chapter 08: VoIP and Network Security Controls
- Chapter 09: Security Framework for Enterprise VoIP Networks
- Chapter 10: Provider Architectures and Security
- Chapter 11: Enterprise Architectures Security





## Contents



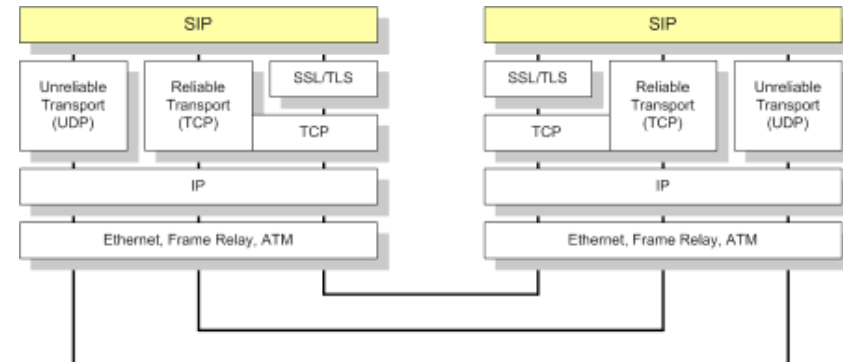
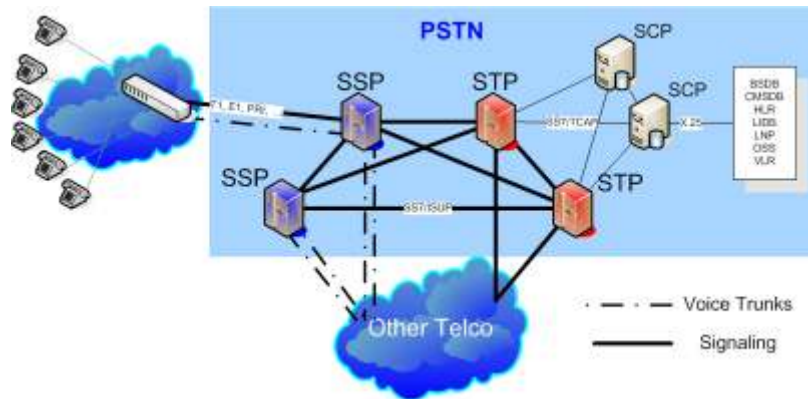
- Chapter 01: はじめに
- Chapter 02: VoIPのアーキテクチャとプロトコル
- Chapter 03: 脅威と攻撃
- Chapter 04: VoIPの脆弱性
- Chapter 05: シグナリング防御のメカニズム
- Chapter 06: メディア防御のメカニズム
- Chapter 07: 鍵管理のメカニズム
- Chapter 08: VoIPとネットワークのセキュリティコントロール
- Chapter 09: エンタープライズVoIPネットワークのセキュリティフレームワーク
- Chapter 10: プロバイダのアーキテクチャとセキュリティ
- Chapter 11: エンタープライズのアーキテクチャとセキュリティ





# 1. Introduction

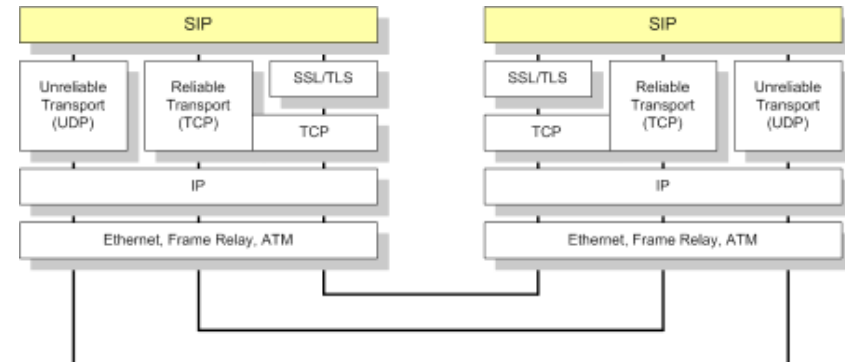
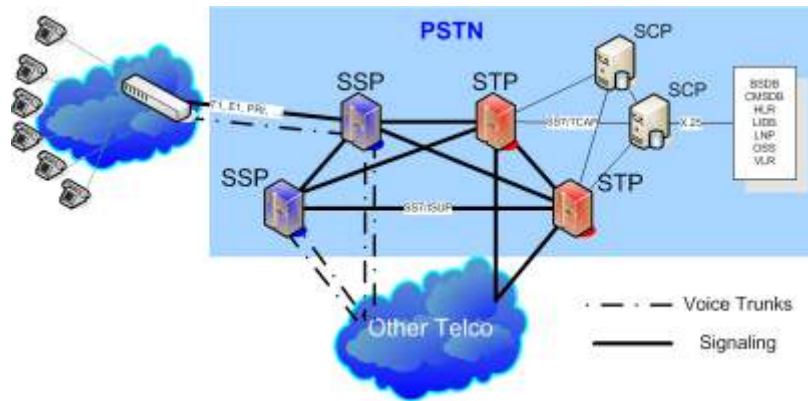
- VoIP is about the transition from the closed PSTN/TDM networks into all-IP telephony





# 1. はじめに

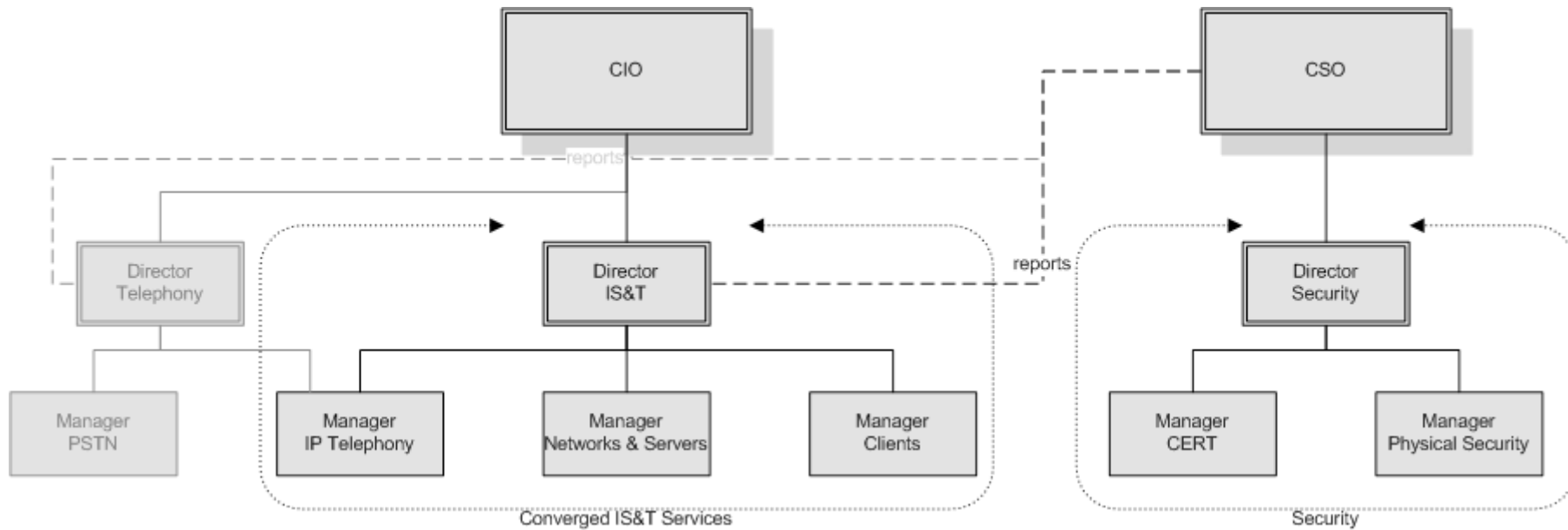
- VoIPとはクローズドなPSTN/TDMネットワークからオールIPテレフォニーへの移行のこと







# 1.1 集中型のIS&Tとセキュリティ組織





## 2.1 VoIP Architectures



- Architectures:
  - Peer-to-Peer
  - PBX/Enterprise VoIP
  - Carrier VoIP
  - Service Provider VoIP
  - Softswitch VoIP
  - IMS VoIP





## 2.1 VoIPのアーキテクチャ



- ・ アーキテクチャ:
  - ・ Peer-to-Peer
  - ・ PBX/エンタープライズVoIP
  - ・ キャリヤVoIP
  - ・ サービスプロバイダVoIP
  - ・ ソフトスイッチVoIP
  - ・ IMS VoIP





## 2.2 VoIP Network Components



- Terminals
  - Soft/hard phone, mobile device, ...
- Call Manager
  - Gatekeeper, Registrar, HSS, HLR, ...
- Signaling Server/Gateway
  - P2P Supernode, IP-PBX, softswitch, CSCF, MGCF
- Media Server/Gateway
  - MGW, MGCF, SBC
- Session Border Elements
  - ALG, VPN, SBC, ...





## 2.2 VoIPネットワークのコンポーネント

- 端末
  - ・ ソフト／ハード電話, モバイルデバイス, ...
- コールマネージャ
  - ・ ゲートキーパー, レジストラ, HSS, HLR, ...
- シグナリングサーバ／ゲートウェイ
  - ・ P2P Supernode, IP-PBX, ソフトスイッチ, CSCF, MGCF
- メディアサーバ／ゲートウェイ
  - ・ MGW, MGCF, SBC
- セッションボーダーエレメント
  - ・ ALG, VPN, SBC, ...





## 2.3 VoIP Protocols



- Signaling:
  - SIP
  - H.323
  - SS7/Sigtran
  - MGCP/H.248
- Media:
  - RTP, RTCP
- Transport:
  - IPv4 and IPv6
  - SCTP
  - TLS
- Others: DHCP, DNS, Diameter, Radius, ...





## 2.3 VoIPプロトコル



- シグナリング:
  - SIP
  - H.323
  - SS7/Sigtran
  - MGCP/H.248
- メディア:
  - RTP, RTCP
- トランスポート:
  - IPv4 と IPv6
  - SCTP
  - TLS
- その他: DHCP, DNS, Diameter, Radius, ...





### 3. VoIP Threats and Attacks



- **Threat:** The means through which someone can do something bad. A potential violation of security.
- **Attack:** The attempt of doing something bad.
- **Exploit:** The tool of conducting something bad.
- **Vulnerability:** The flaw or weakness that enables threats, attacks or exploits.





### 3. VoIPの脅威(Threats)と攻撃(Attacks)

- ・ 脅威(Threat): 誰かが悪いことをする 方法. セキュリティへの 潜在的な 侵害.
- ・ 攻撃(Attack): 悪いことをしようとする 試み.
- ・ イクスプロイト(Exploit): 悪いことをするための ツール.
- ・ 脆弱性(Vulnerability): 脅威、攻撃、イクスプロイトを可能にしてしまう 欠陥や弱点.

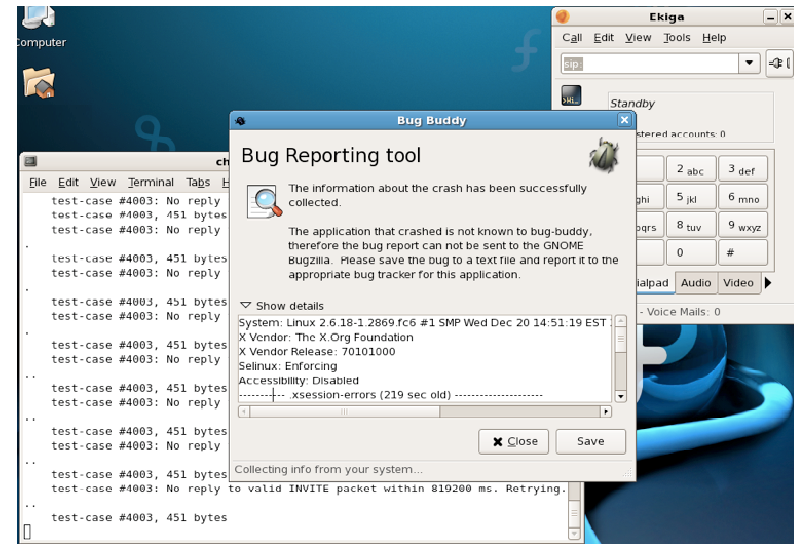




## 3.1 VoIP Threat and Attack Categories



- Service disruption and annoyance
- Eavesdropping and traffic analysis
- Masquerading and impersonation
- Unauthorized Access
- Fraud

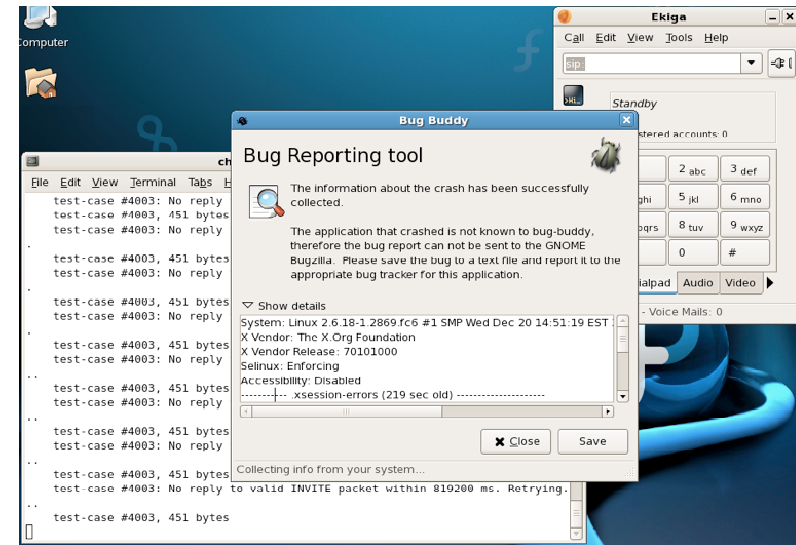




## 3.1 VoIPの脅威と攻撃のカテゴリ



- ・ サービスの途絶と妨害
- ・ 盗聴とトラフィック解析
- ・ なりすましと偽装
- ・ 不正アクセス
- ・ 詐欺





## 3.2 Service Disruption and Annoyance



- Malformed packets DoS attack
  - Found by e.g. fuzzing
  - Caused by broken inputs, malformed packets
  - Buffer overflow is an example where malformed packets can be used to get full access to the device
  - 70% of all known vulnerabilities appear to be in this category
- Load-based flooding attacks (DDoS)
  - Performance flaw, or load balancing problem
- SPIT
  - Hard in real-time communications
  - Phone rings before the unwanted media can be detected
  - Black-lists and white-lists





## 3.2 サービスの途絶と妨害

- 不正なパケットのDoS攻撃
  - ・ 例えばファジングによって検出される
  - ・ 壊れた入力や、不正なパケット
  - ・ バッファオーバーフローは、不正なパケットがデバイスへのフルアクセスに使用され得る例
  - ・ 知られている脆弱性の70%はこのカテゴリに入る
- 負荷ベースのフラッディング攻撃 (DDoS)
  - ・ パフォーマンスの欠陥またはロードバランスの問題
- SPIT
  - ・ リアルタイムコミュニケーションにおいては厳しい
  - ・ 不要なメディアが検出される前の呼び出し音
  - ・ ブラックリストとホワイトリスト





### 3.3 VoIP Fuzzing



- The Denial of Service attack can also consist of individual malformed packets
- The process of generating malformed packets randomly or semi-randomly is called fuzzing
- In 2002, PROTOS researchers from University of Oulu released a freely available test suites for SIP and H.323
  - Uses a small set of efficient tests instead of randomly generating millions of malicious packets
- Codenomicon released commercial tools for use in VoIP penetration testing and quality assurance





### 3.3 VoIPファジング

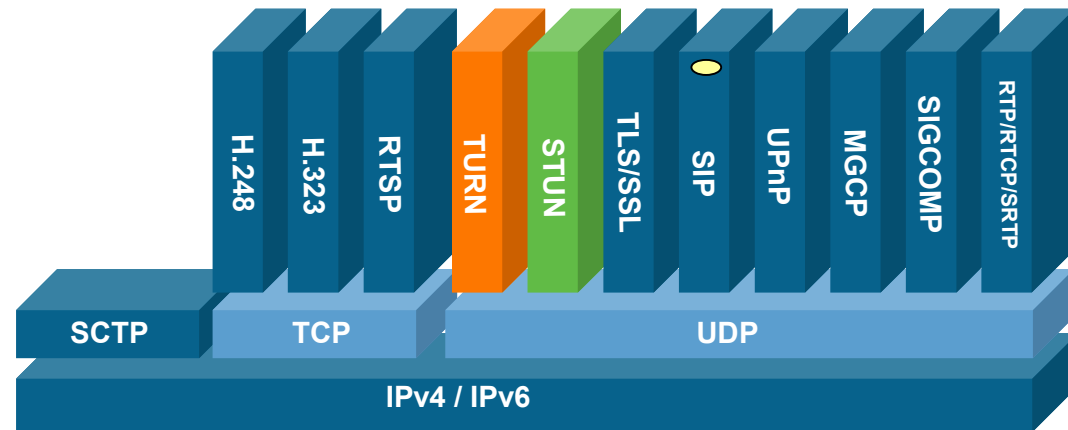


- Denial of Service攻撃は、個々の不正パケットから構成されることがある
- ランダムまたはセミランダムに不正なパケットを生成することをファジングと呼ぶ
- 2002年、Oulu大学のPROTOSの研究者がフリーで入手可能なSIPとH.323のテストスイートをリリース
  - ・ ランダムに生成する数百万の悪意のあるパケットの代わりに効果的な小規模のテストを使用
- CodenomiconはVoIPペネトレーションテストと品質保証に使用するためのツールをリリース





## 3.4 Fuzzing Interfaces

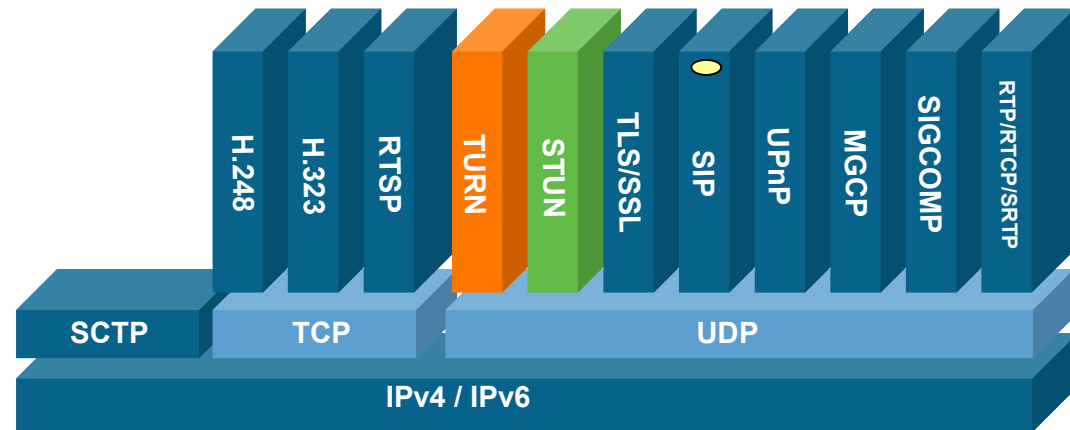


- VoIP devices and services need to be tested on all layers
- Any protocol interface that is open to the public Internet is a high risk to the system
- 80% of all VoIP devices still crash when tested with fuzzing





## 3.4 ファジングインターフェース

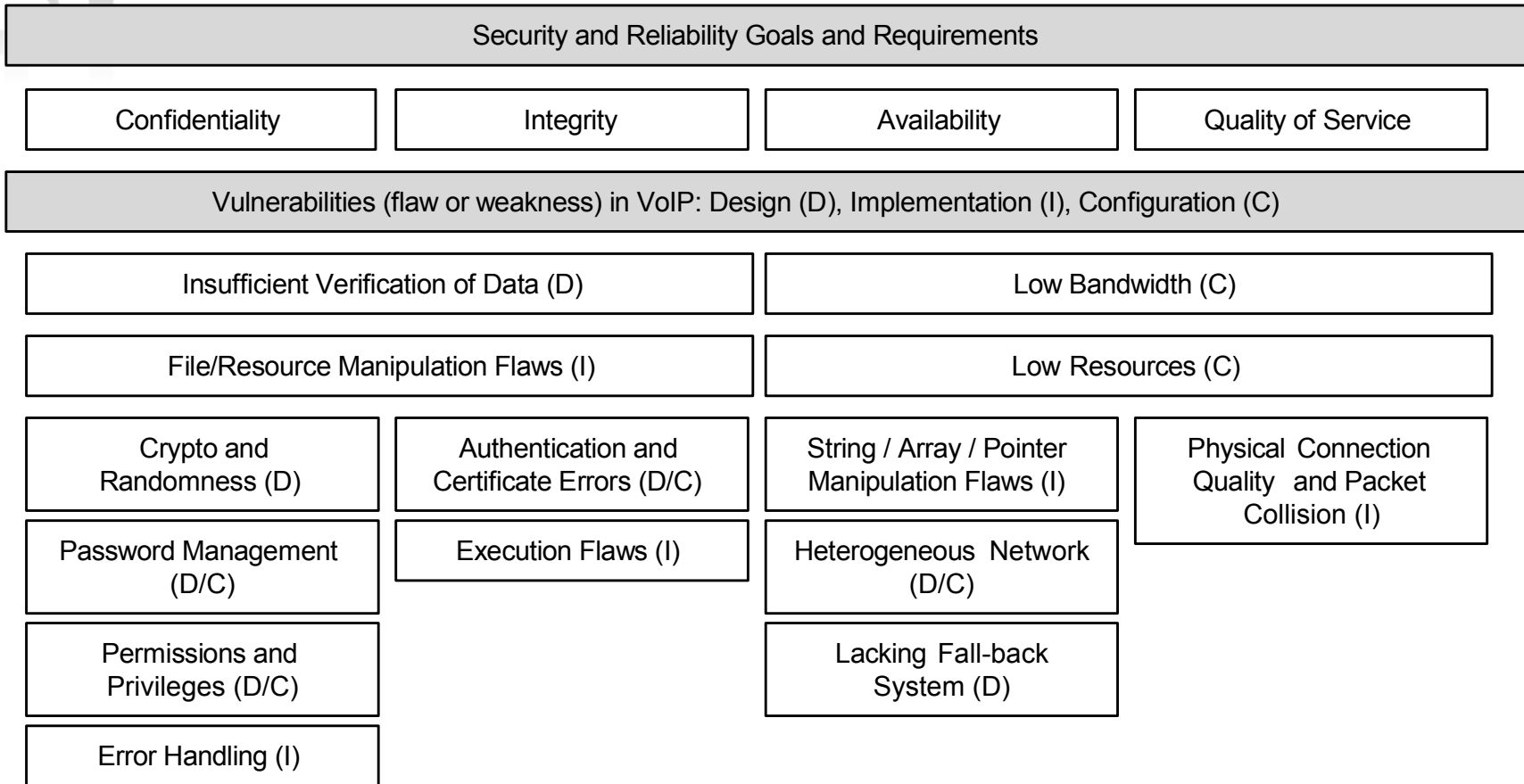


- VoIPデバイスとサービスは、全てのレイヤにわたってテストする必要がある
- 公衆インターネットに開かれているあらゆるプロトコルインターフェースは、システムにとって大きなリスクとなる
- VoIPデバイスの80%はファジングによってクラッシュする



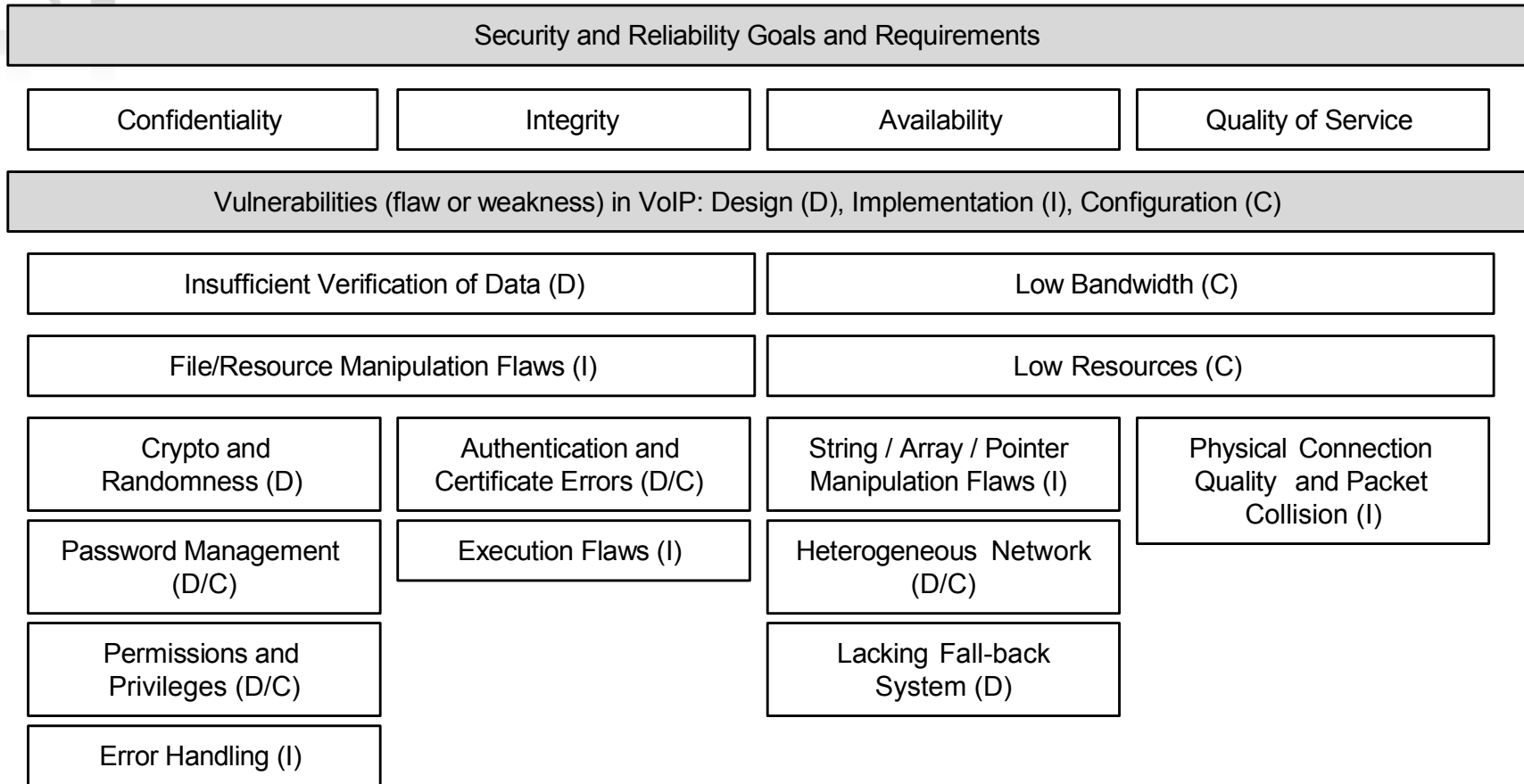


# 4. VoIP Vulnerabilities





# 4. VoIPの脆弱性



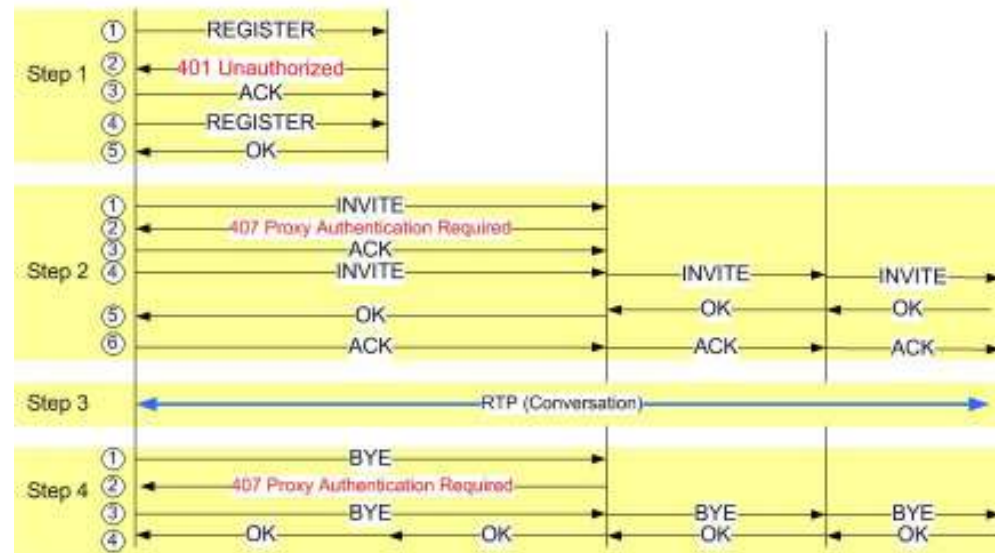
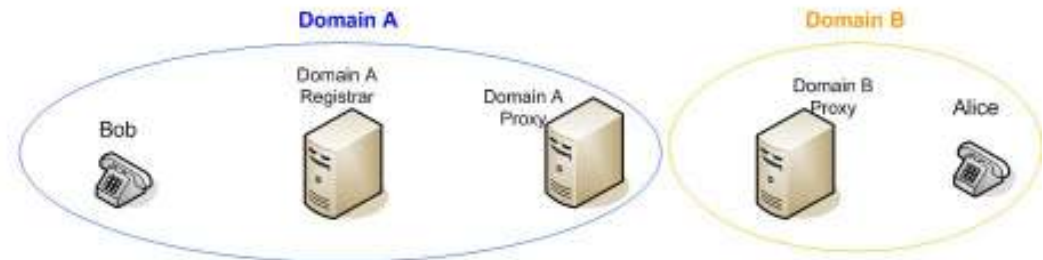


# 5. Signaling Protection Mechanisms

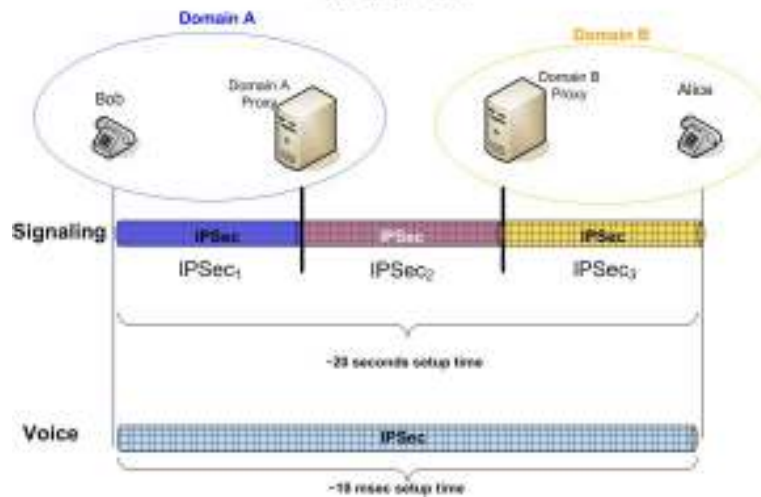


- Authentication
- Encryption
  - TLS
  - DTLS
  - S/MIME
  - IPSEC

SIP Registration and Call Authentication



SIP and IPsec



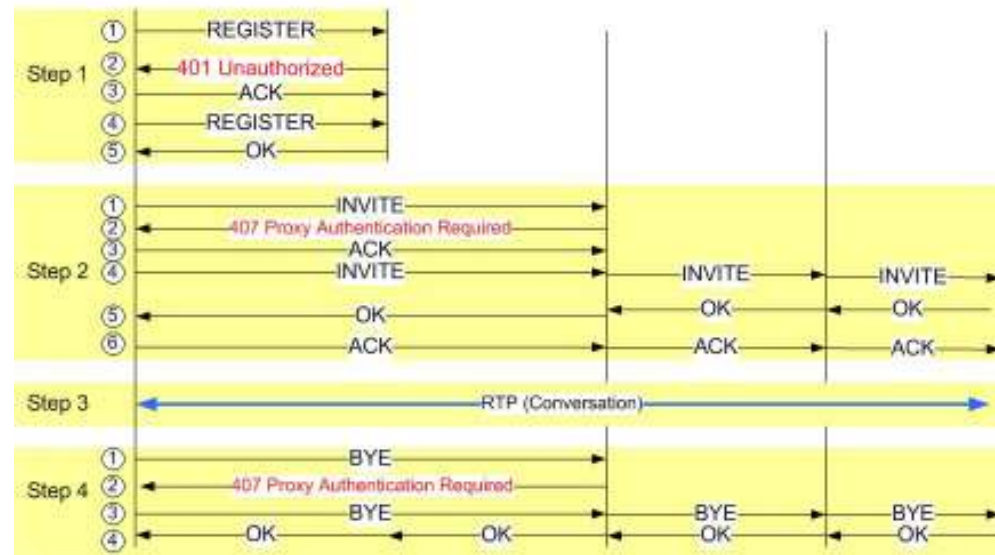
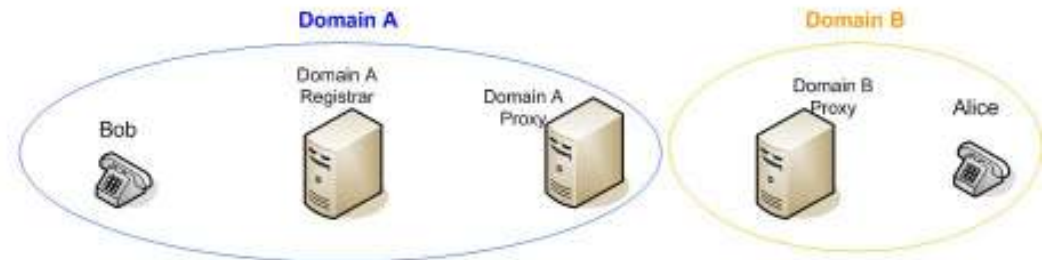


# 5. シグナリング防御のメカニズム

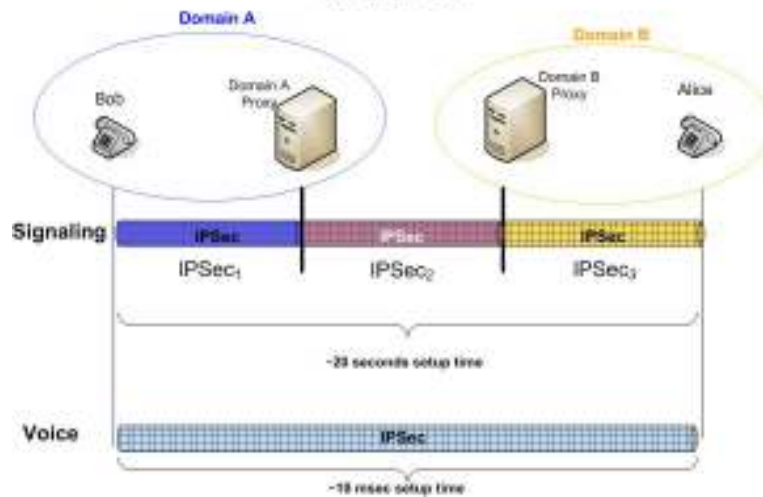


- 認証
- 暗号化
  - TLS
  - DTLS
  - S/MIME
  - IPSEC

SIP Registration and Call Authentication

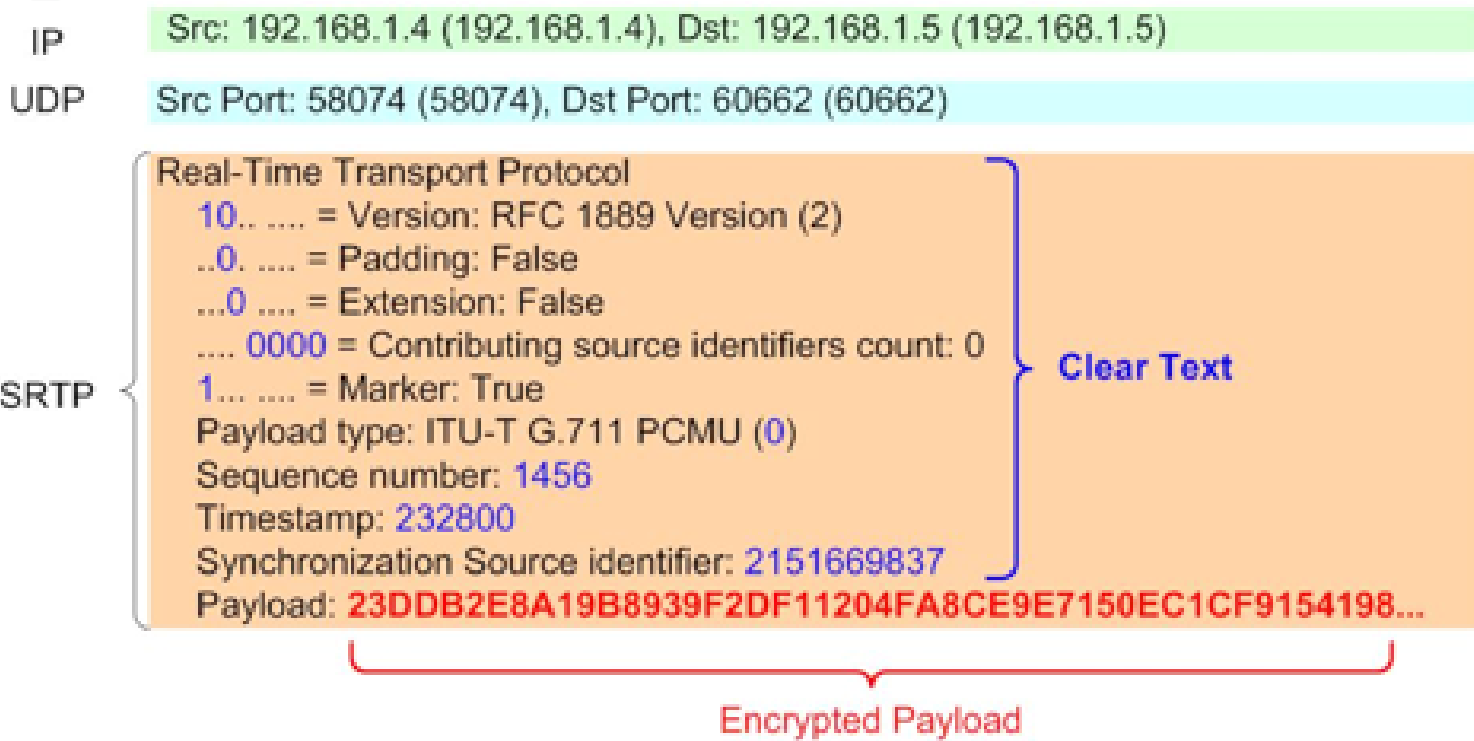


SIP and IPsec



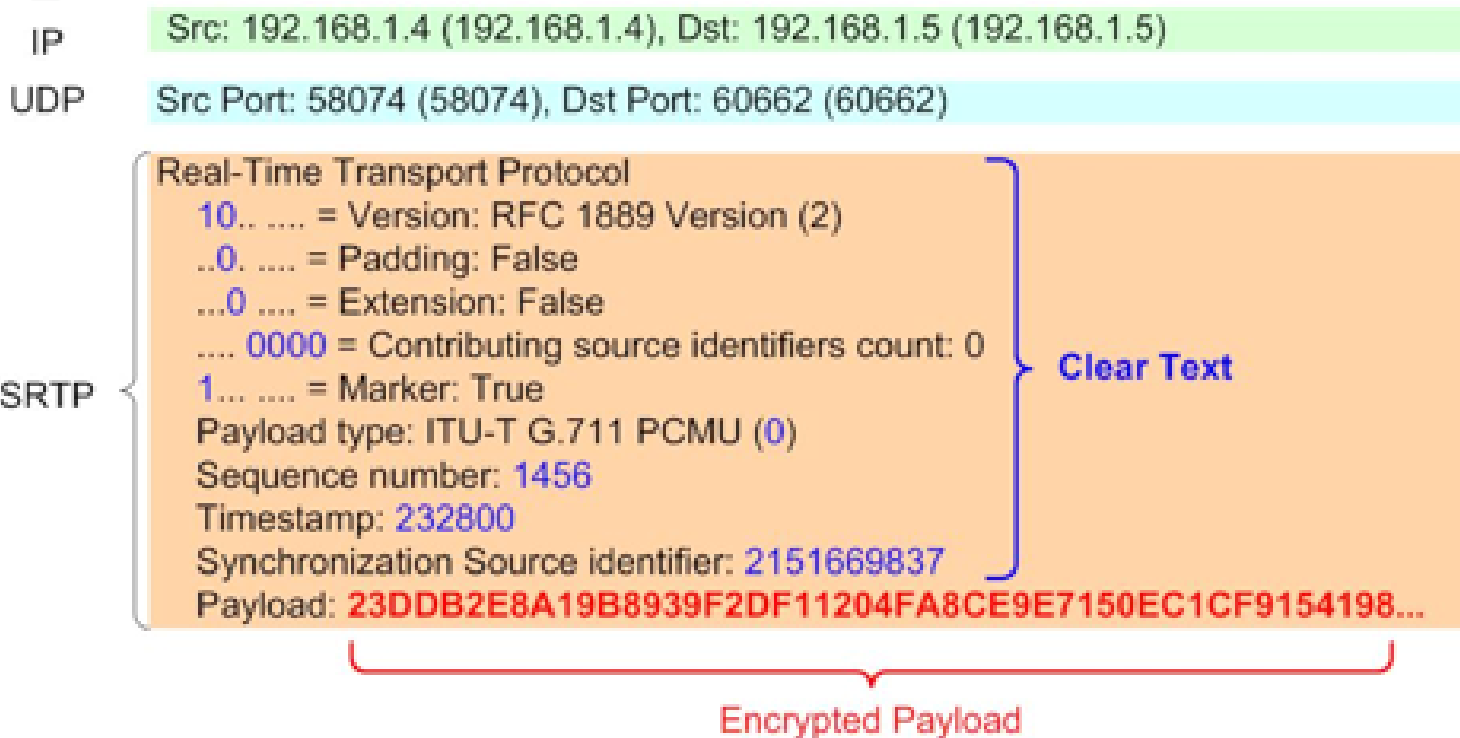


# 6. Media Protection Mechanisms





## 6. メディア防御のメカニズム





## 7. Key Management



- Challenging to design and implement correctly
- The IETF RFC 4046 “MSEC Group Key Management Architecture” defines an architecture which consists of abstractions and design principles for developing key management protocols.
- MIKEY
- ZRTP
- SDEScriptions
- IKE
- Additional mechanisms are being discussed in IETF





## 7. 鍵管理



- 正しくデザインし実装するのが難しい
- IETF RFC 4046 “MSEC Group Key Management Architecture”では、鍵管理のプロトコルを開発するための概念とデザインの原理からなるアーキテクチャを定義している。
- MIKEY
- ZRTP
- SDEScriptions
- IKE
- IETFでは更なるメカニズムが議論されている

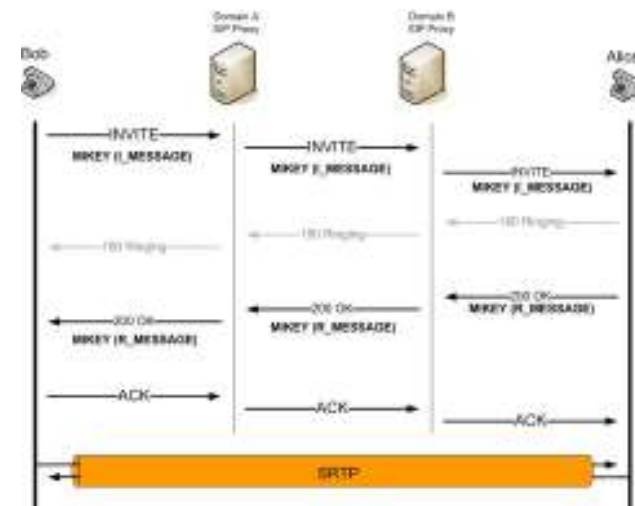




# 7.1 Key Management Mechanisms (MIKEY)



- MIKEY
  - The protocol should **maintain simplicity** for ease of implementation, performance and security.
  - Minimize message exchange**; the negotiation of key material should be accomplished in one round trip.
  - Support secure end-to-end key management.**
  - Protocol integration**; allow transport of messages within other protocols (i.e. SDP)
  - Protocol independence**; maintain independence from any security functionality imposed by the underlying transport.
  - Low bandwidth** consumption and low computational workload.





## 7.1 鍵管理のメカニズム (MIKEY)



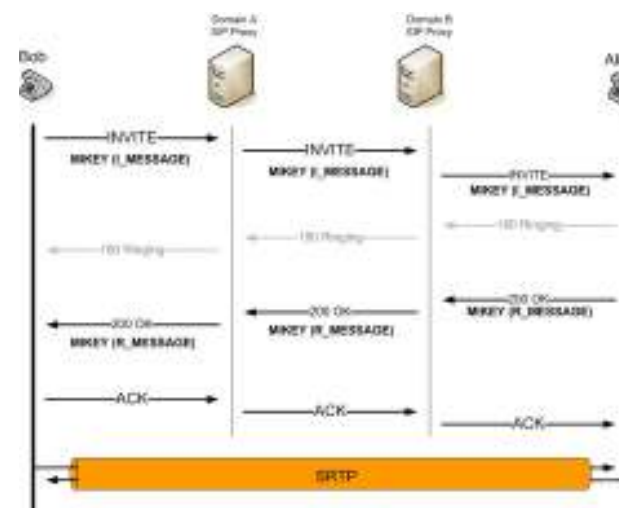
### MIKEY

- 実装の簡便性、パフォーマンス、セキュリティのため、**プロトコルはシンプルであるべき。**
- **メッセージ交換は最小にする**; 鍵関連のネゴシエーションは、一つのラウンドトリップでなされるべき。
- **エンドツーエンドでセキュアな鍵管理のサポート。**
- **プロトコルの統合**; 他のプロトコル内でのメッセージの送信(例: SDP)
- **プロトコルの独立**; 下位のトランスポートのセキュリティ機能からの独立を保つ。
- **低い帯域消費**と低い計算負荷。

MIKEY COMMON HEADER PAYLOAD

1								2								3															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
VERSION								DATA TYPE								NEXT PAYLOAD								V PRF FUNCTION							
CSB ID																															
#CS								CS ID MAP TYPE								CS ID MAP INFO															

VERSION	8 - bits, the version number of MIKEY, currently (w)1 as defined in RFC 3630
DATA TYPE	8 - bits, describes the type of message (e.g. public key transport, verification, error message)
NEXT PAYLOAD	8 - bits, identifies the payload that is added after this payload
V	1 - bit, flag to indicate whether a verification message is expected or not. Typically this is set by the initiator of a message only.
PRF FUNCTION	7 - bits, indicates the PRF function that has been (or will be) used for key derivation
CSB ID	32 - bits, identifies the CSB
#CS	8 - bits, indicates the number of Crypto Sessions that will be handled within the CSB. Although it is possible to have 255 CS's it is not likely that will occur in a single CSB. The number 0 indicates that no CS is included.
CS ID MAP TYPE	8 - bits, specifies the method of uniquely mapping Crypto Sessions to the security protocol sessions
CS ID MAP INFO	16 - bits, identifies the crypto session(s) for which the SA should be created. Currently the defined map is SRTP-ID.

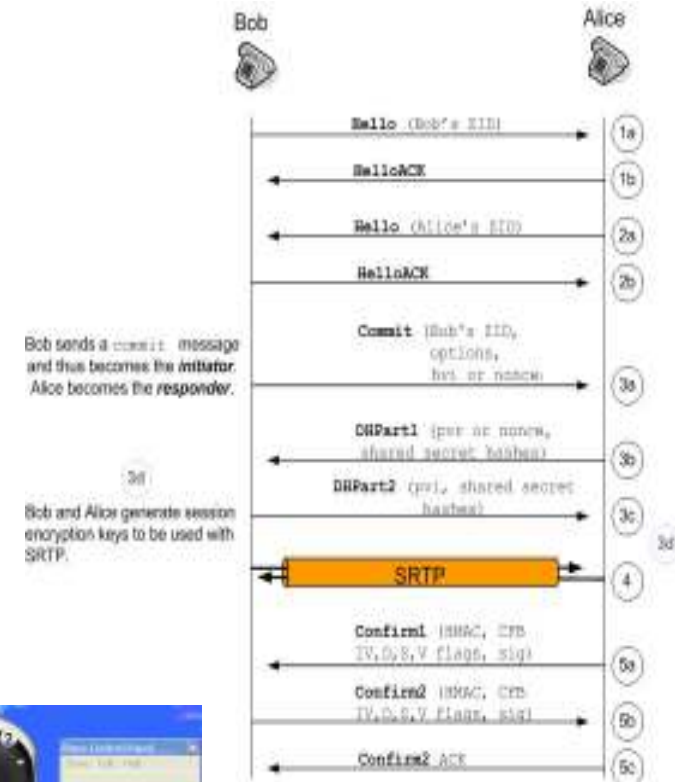




## 7.2 Key Management Mechanisms (ZRTP)



- ZRTP
  - Key exchange through the media path
  - Provides end-to-end key negotiation and avoids intermediaries
  - Is not impacted by NAT
  - Ideal for peer-to-peer
  - Implemented by several vendors



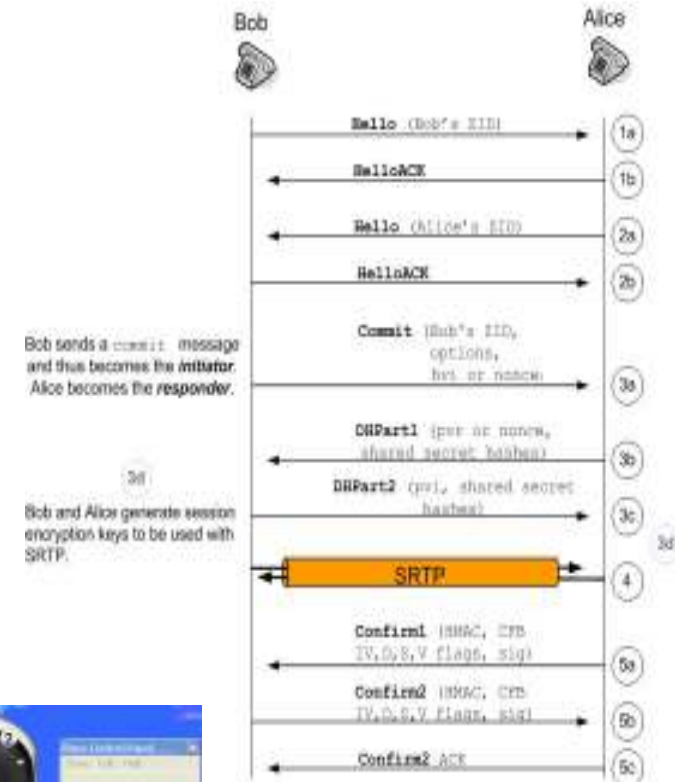


## 7.2 鍵管理のメカニズム (ZRTP)



### ・ ZRTP

- ・ メディアパス上での鍵交換
- ・ エンドツーエンドの鍵ネゴシエーションを提供し、仲介を必要としない
- ・ NATに影響されない
- ・ ピアツーピアに理想的
- ・ 複数のベンダが実装





## 7.3 Key Management Mechanisms (SDEScriptions)



- SDEScriptions
  - Key exchange through signaling
  - Requires signaling to be encrypted (TLS)
  - Some vendor implementations
  - Key exchange requires intermediaries

```
SIP Portion of SIPS message {
  INVITE sip:alice@domain-b.com:5061 SIP/2.0
  Via: SIP/2.0/TLS 192.168.1.3:5061;branch=z9hG4bK-d04dcaal
  From: bob<sips:bob@domain-a.com:5061>;tag=aed516f97e1da529c0
  To: <sips:alice@domain-b.com:5061>
  Call-ID: ceab1739-db25a1e9@192.168.1.3
  CSeq: 102 INVITE
  Max-Forwards: 70
  Contact: bob<sips:bob@domain-a.com:5061>
  Expires: 240
  User-Agent: 001217E57E31 Linksys/RT31P2-3.1.6(LI)
  Content-Length: 335
  Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
  Content-Type: application/sdp
}

SDP Portion of SIPS Message {
  v=0
  o=bob 2890844526 2890842807 IN IP4 192.168.1.3
  s=VoIP Security Testing
  i=Develop Methodology for VoIP Security Testing
  e=bob@domain-a.com (Bob The Security Guy)
  c=IN IP4 161.44.17.12/127
  t=2873397496 2873404696
  m=audio 51442 RTP/SAVP 0
  a-crypto:1 AES_CM_128_HMAC_SHA1_32
           inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2*20|1:32
}

```

crypto:1 AES\_CM\_128\_HMAC\_SHA1\_32 inline:UhbLIINTNw3bIKHQVLQze6oHsyF4jGj3NheKoYx|2\*20|1:4

Media Attribute (a): crypto:





## 7.3 鍵管理のメカニズム (SDEScriptions)



### • SDEScriptions

- シグナリングを通じての鍵交換
- シグナリングが暗号化される必要がある (TLS)
- いくつかのベンダが実装
- 鍵交換に仲介が必要

```
SIP Portion of SIPS message
INVITE sip:alice@domain-b.com:5061 SIP/2.0
Via: SIP/2.0/TLS 192.168.1.3:5061;branch=z9hG4bK-d04dcaal
From: bob<sips:bob@domain-a.com:5061>;tag=aed516f97e1da529c0
To: <sips:alice@domain-b.com:5061>
Call-ID: ceab1739-db25a1e9@192.168.1.3
CSeq: 102 INVITE
Max-Forwards: 70
Contact: bob<sips:bob@domain-a.com:5061>
Expires: 240
User-Agent: 001217E57E31 Linksys/RT31P2-3.1.6(LI)
Content-Length: 335
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
Content-Type: application/sdp

SDP Portion of SIPS Message
v=0
o=bob 2890844526 2890842807 IN IP4 192.168.1.3
s=VoIP Security Testing
i=Develop Methodology for VoIP Security Testing
e=bob@domain-a.com (Bob The Security Guy)
c=IN IP4 161.44.17.12/127
t=2873397496 2873404696
m=audio 51442 RTP/SAVP 0
a-crypto:1 AES_CM_128_HMAC_SHA1_32
         inline:NzB4d1BINUAwLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2*20|1:32
```

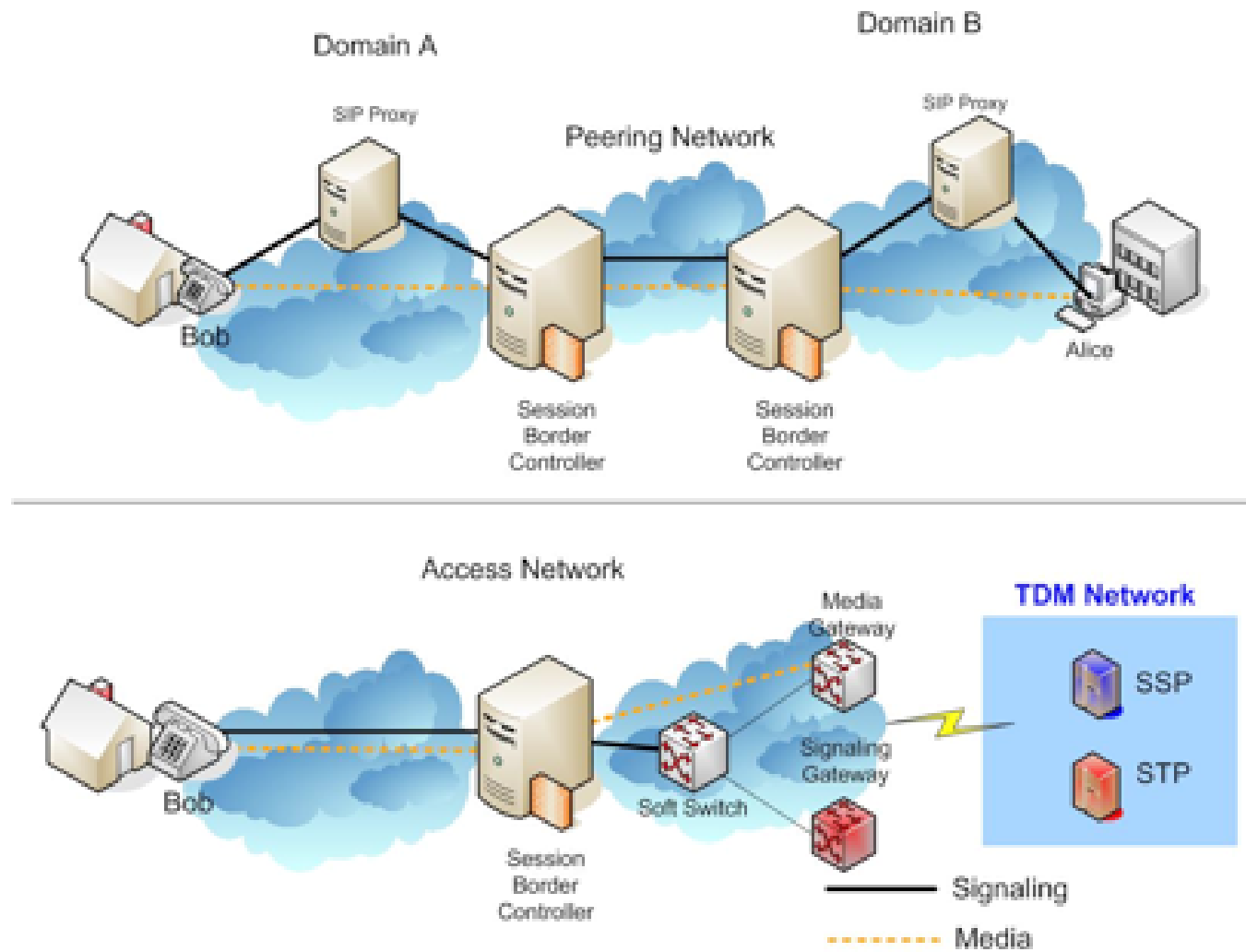
crypto:1 AES\_CM\_128\_HMAC\_SHA1\_32 inline:UhbLIINTNw3bIKHQVLQze8oHsyF4jGj3NheKoYx|2\*20|1:4

Media Attribute (a): crypto:



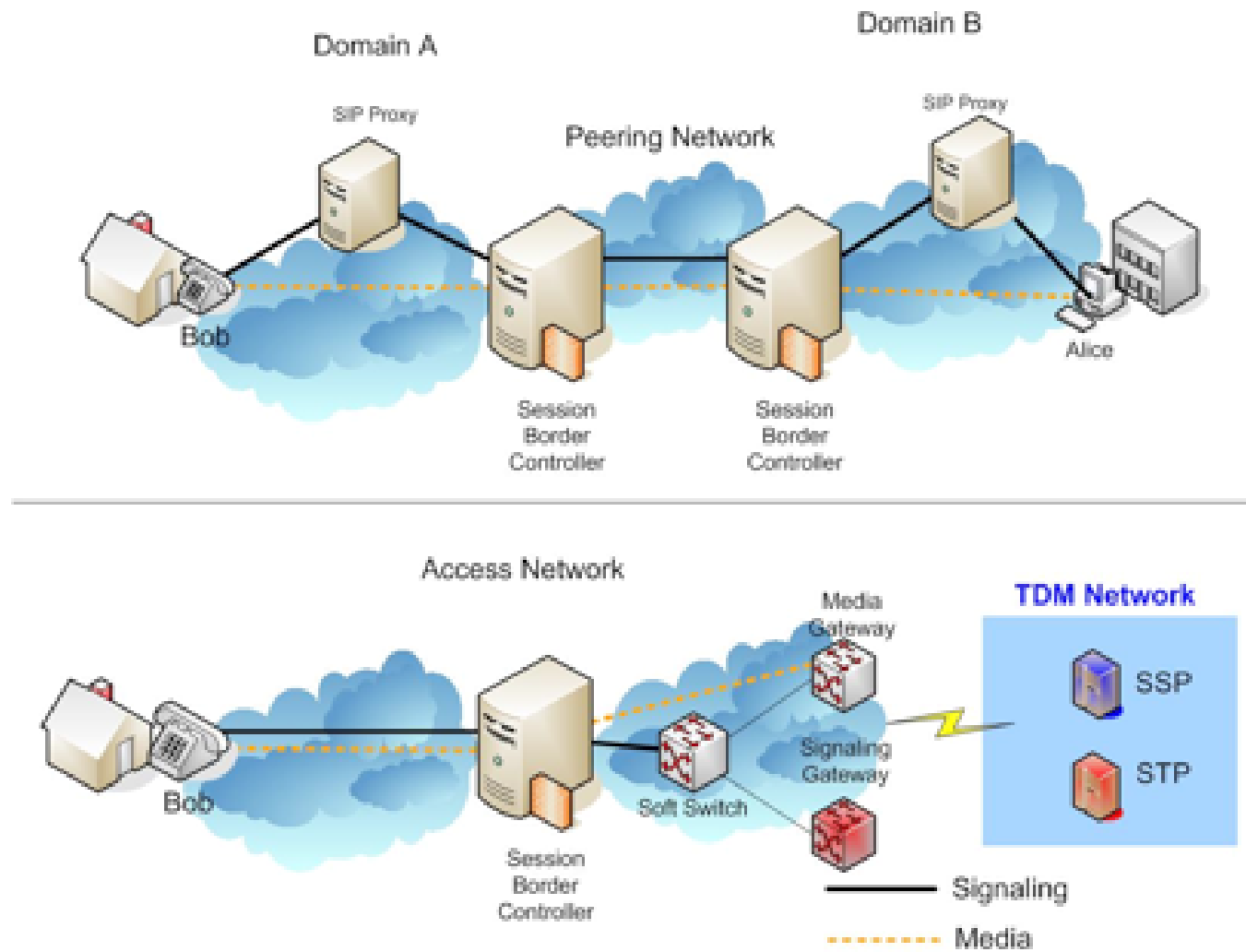


## 8. VoIP and Network Security Controls





## 8. VoIPとネットワークのセキュリティコントロール





## 9. Security Framework for Enterprise VoIP Networks



- ISO 17799/27001, Information Security Management Requirements
- Mapped VoIP controls
- Addresses other regulatory requirements
  - SOX
  - GLBA
  - SAS70
- Security Policy
- External Parties
- Asset Management
- Physical and environmental security
- Operations management
- Access Control
- System Acquisition, development and maintenance
- Incident management
- Business Continuity
- Compliance





## 9. エンタープライズVoIPネットワークのセキュリティ フレームワーク

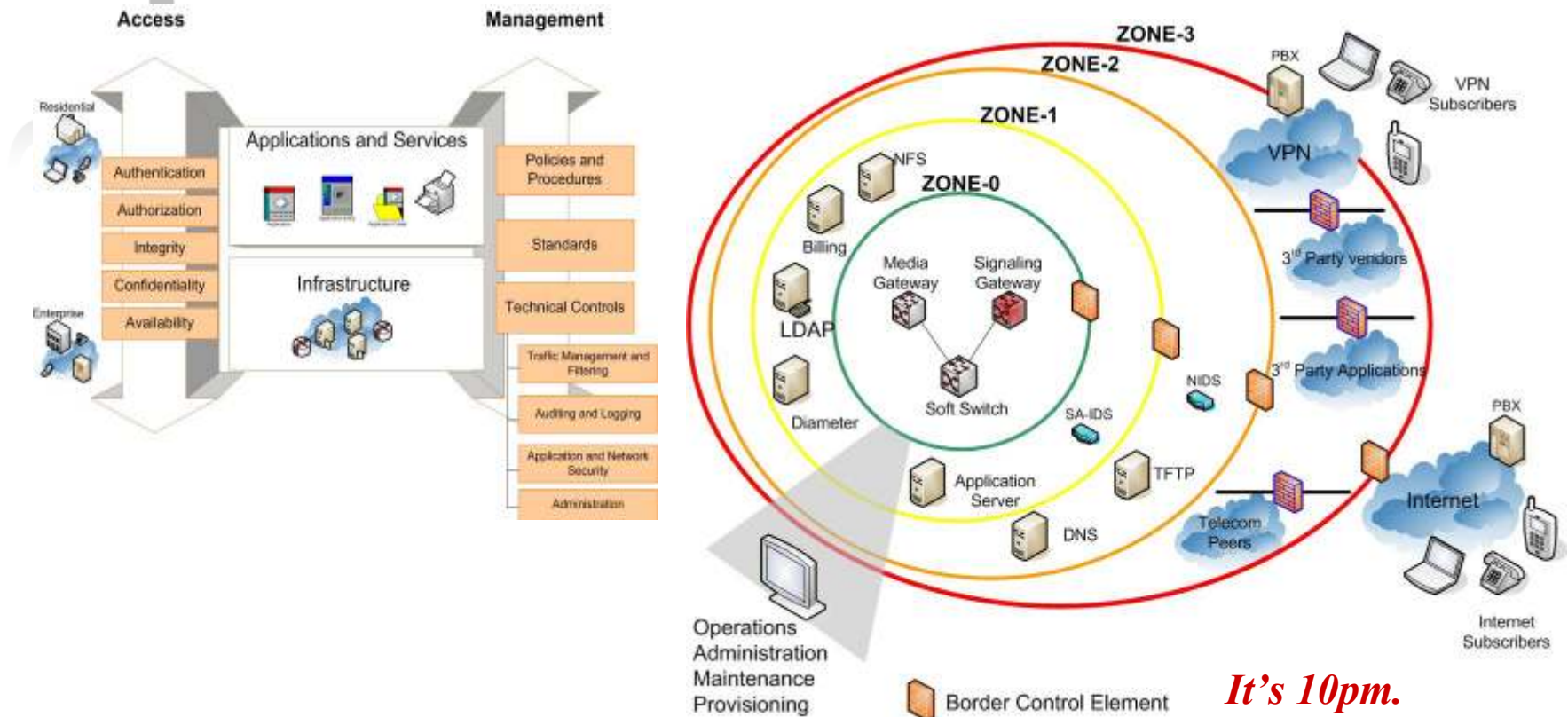


- ISO 17799/27001, Information Security Management Requirements
- VoIP管理にマップされる
- 他の規制基準へのアドレス
  - SOX
  - GLBA
  - SAS70
- セキュリティポリシー
- 外部団体
- 資産管理
- 物理的及び環境のセキュリティ
- 運用管理
- アクセス制御
- システムの取得、開発、保守
- インシデント管理
- ビジネスの継続
- コンプライアンス





# 10.1 Provider Architectures and Security

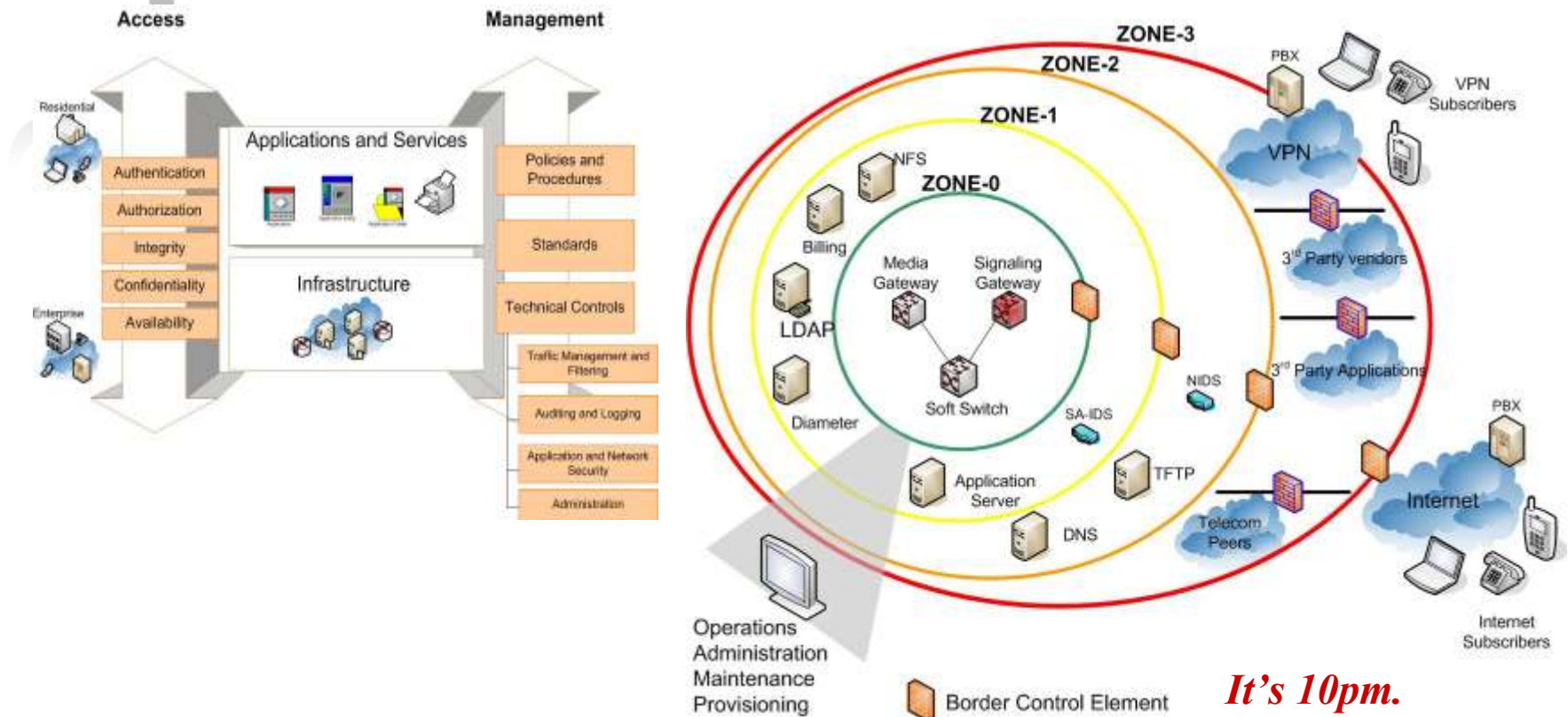


*It's 10pm.  
Do you know if your  
SBC has been  
configured properly?*





# 10.1 プロバイダのアーキテクチャとセキュリティ



*It's 10pm.  
Do you know if your  
SBC has been  
configured properly?*





## 10.2 Provider Architectures and Security



- Summary of lesson's learned from assessing carrier grade environments:
  - Some signaling/media attacks are not managed properly. Call flow manipulation attacks
  - Lack of adequate monitoring capabilities on core components (i.e., SBC's, gateways, soft-switch etc.).
  - Attacks originating from peering points are not properly managed (i.e. Enterprise customers and carriers)
- Recommendations
  - Plan early and ask questions. Poor security architecture and design requirements lead to many mistakes that can be prevented.
  - Evaluate critical network elements (i.e. SBC's signaling gateways etc.) using a multidimensional approach (not just lab "xyz" run nmap/Nessus on my box).





## 10.2 プロバイダのアーキテクチャとセキュリティ



- ・ キャリヤグレードの環境から得られた教訓:
  - ・ シグナリング／メディアへの攻撃が適切に管理されていない. コールフローのマニピュレーション攻撃
  - ・ コアのコンポーネントに対する十分なモニタ機能の欠如 (すなわち、SBC, ゲートウェイ、ソフトスイッチ等).
  - ・ ピアリングポイントから送信される攻撃が正しく管理されていない (すなわちエンタープライズの顧客とキャリヤ)
- ・ 推奨
  - ・ 早めに計画し、疑問をもつ. 粗末なセキュリティアーキテクチャとデザイン仕様は避けることのできる多数の誤りにつながる.
  - ・ 多次元のアプローチを使用して(単にラボ“xyz”が nmap/Nessus を実行するのではなく)重要なネットワークエレメント(SBCやシグナリングゲートウェイ等)を評価する.

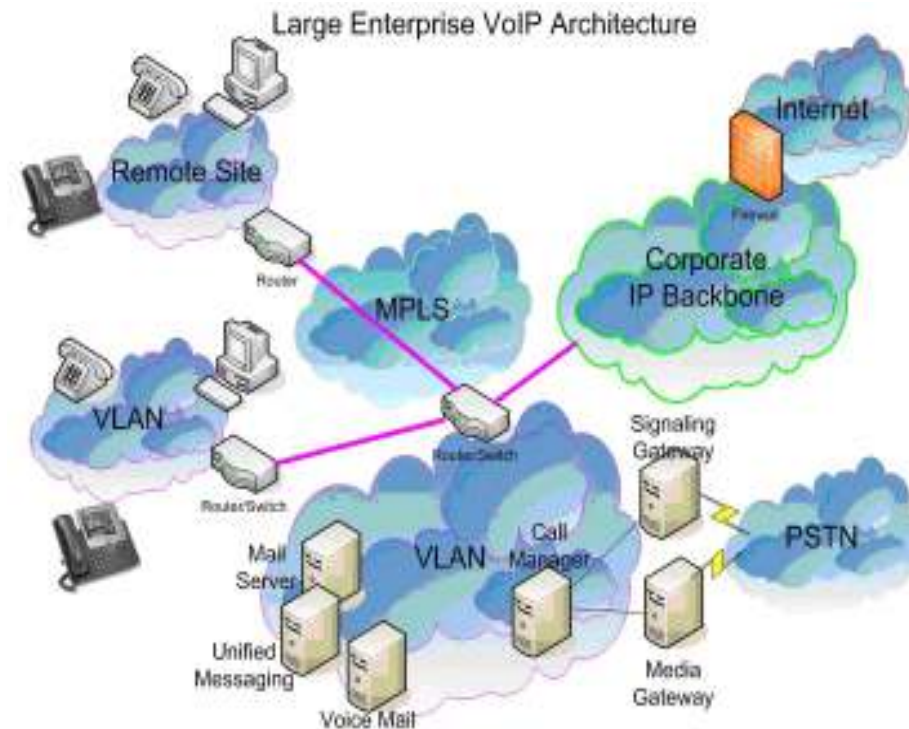




# 11. Enterprise Architectures Security



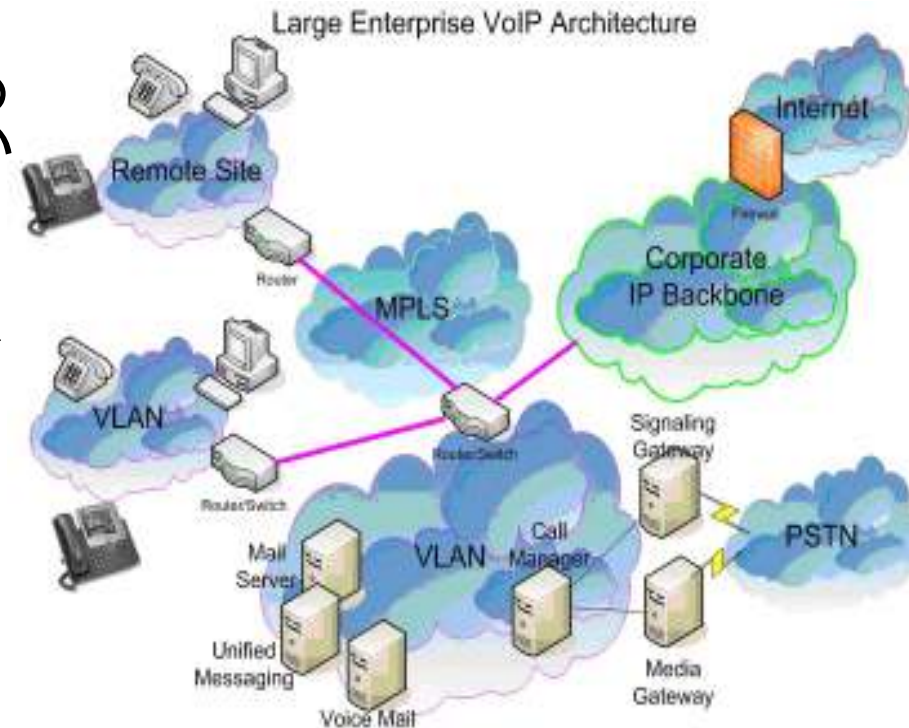
- Areas where most common weaknesses found in assessments
  - No adequate protection for signaling or media
  - Poor ACL's/Network filtering
  - Improperly configured systems
  - Outdated software versions
- Most weaknesses are based on poor or lack of security requirements.



## 11. エンタープライズアーキテクチャのセキュリティ



- ・ 評価によって一般的な弱点が見つかるエリア
  - ・ シグナリングやメディアのための十分な防御がない
  - ・ 粗末なACL/ネットワークフィルタリング
  - ・ 不適切に設定されたシステム
  - ・ 古いソフトウェアバージョン
- ・ ほとんどの弱点はセキュリティ要求が粗末であるか、欠如していることが原因.





## Summary



- VoIP security is not only about security mechanisms
- For full security analysis, you should study:
  - Threats
  - Attacks
  - Vulnerabilities
  - Architectures
  - Countermeasures
- There is no one way of doing it right, different techniques apply for different needs
- Security is a process not a product!





## まとめ



- ・ VoIPのセキュリティは、セキュリティメカニズムに関することだけではない
- ・ 十分なセキュリティの解析のために以下のことを学ぶべき:
  - ・ 脅威(Threats)
  - ・ 攻撃(Attacks)
  - ・ 脆弱性(Vulnerabilities)
  - ・ アーキテクチャ(Architectures)
  - ・ 対応策(Countermeasures)
- ・ うまくいく単一の方法はない, 様々な要求に様々な技術を適用する
- ・ セキュリティはプロセスであり製品ではない!





## Author's contacts



Ari Takanen

Codonomicon

[ari.takanen@codonomicon.com](mailto:ari.takanen@codonomicon.com)

Tel: +358-40-5067678

[www.codonomicon.com](http://www.codonomicon.com)

Peter Thermos

Palindrome

[peter.thermos@palindrometech.com](mailto:peter.thermos@palindrometech.com)

Tel: +1 (732) 688 0413

[www.palindrometech.com](http://www.palindrometech.com)





## Author's contacts



Ari Takanen

Codonomicon

[ari.takanen@codonomicon.com](mailto:ari.takanen@codonomicon.com)

Tel:+358-40-5067678

[www.codonomicon.com](http://www.codonomicon.com)

Peter Thermos

Palindrome

[peter.thermos@palindrometech.com](mailto:peter.thermos@palindrometech.com)

Tel: +1 (732) 688 0413

[www.palindrometech.com](http://www.palindrometech.com)

