VoIP Security, Integration, and Innovation

Navidut Tauhid

UCC Consultant and Cloud Architect

https://www.linkedin.com/in/naveedtauheed/

Overview

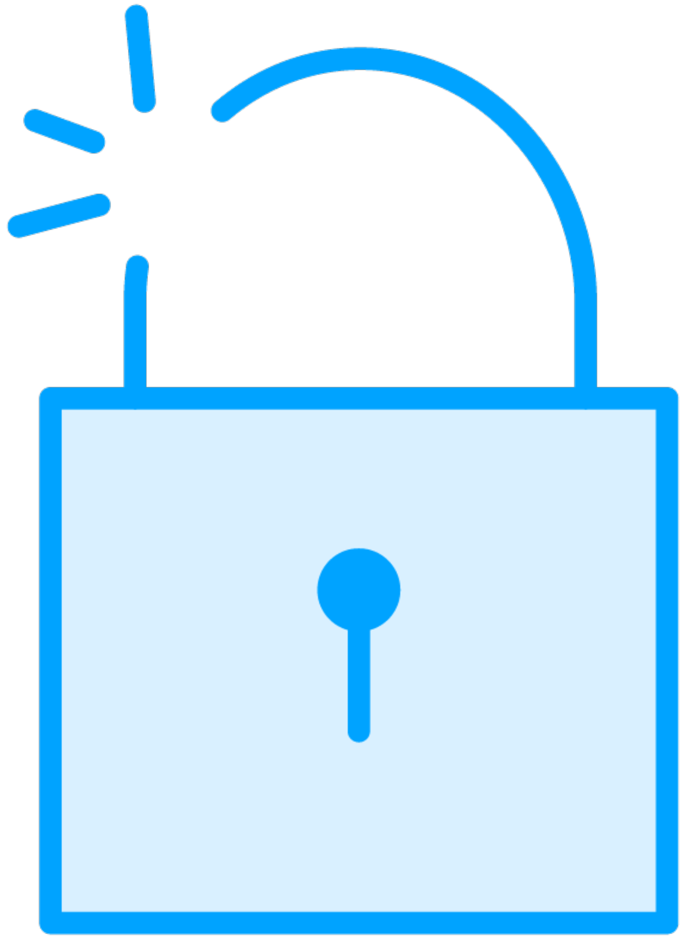
VoIP security

- Different attacks
- Security measures

Integration of VoIP with other technologies

Emerging trends and technologies in VoIP

VoIP Security



Penetration from any component

Security on all devices:

- IP phone
- Microsoft Teams, Cisco WebEx
- Cisco unified communication manager
- TFTP server
- Microsoft Teams cloud
- Network between clients and servers

Devices:

- Switch router or gateway
- Firewall

Eavesdropping and Sniffing or Snooping

Intercepting recording and listening to calls

Stealing sensitive information

Confidential and valuable information

Eavesdropping and Sniffing or Snooping

Financial institutions

Professional services firms

Government agencies

Valuable data

Eavesdropping and Sniffing or Snooping

Call centers

Health records

Payment card data

Treasure trove

Eavesdropping and Sniffing or Snooping

- Infiltrate network
- Obtain sensitive business or financial information
- Sold to competitors

Eavesdropping Protection

Secure protocols

Microsoft Teams

Mutual TLS (MTLS), Oauth

Within Microsoft 365 and Office 365

TLS from clients to services

All network traffic is encrypted

Difficult or impossible to achieve

TLS authenticates and encrypts

The attacker can not read encrypted traffic

Spoofing Attacks

Attacker calls from different number

Tricking the recipient

Confidential information

Spoofing Attacks

Alternate TFTP server

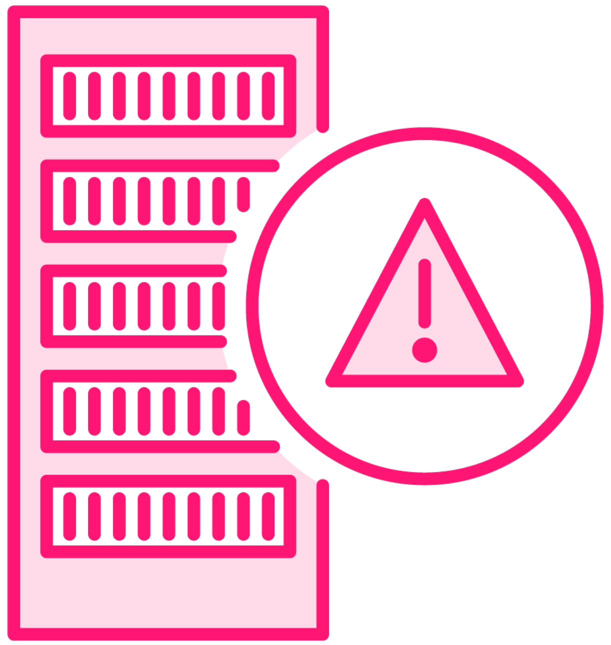
Sends a configuration file of the IP phone

Gathers network information

Connect to the internal network

Denial of Service (DoS) Attacks

Mastermind hacker



Communication system down

DDoS attack on the servers

Distributed Denial of Service (DDoS) Attacks

Disguise as a user

- Initiate a call
- Numerous fake INVITE requests
- Server tries to authenticate
- Computational power and memory

Flood continues

- Server becomes not-responsive
- No legitimate calls
- Unable to communicate
- SIP protocol and UDP
- Flood of specially crafted packets
- Unprotected VoIP server

DDoS Protection

Protecting VoIP

Malicious attacks

Requires

Multi-layered defense strategy

DDoS Protection

Secure communication

Access level control

IP address learning

Media packet policing

DDoS Protection

Authorized and trusted IP addresses

ACL policing

Only trusted peers are allowed

IP address learning
media packets match negotiated SIP/SDP signaling

DDoS Protection

Prioritize authenticated sources

- Priority-aware packet policing
- Limit bandwidth usage
- Application-level call admission control.

Shield sensitive information

- Smooth functioning

Voicemail Hacking

Voicemail box holds confidential information

Hacker can make multiple attempts

Listen to voicemail

International calls

Voicemail Protection

Simple measures

Protect from prying eyes

Strict voicemail password

Complex passwords

Change password

Default or repetitive password

Voicemail Protection

Restrict outgoing calls

Only authorized calls

Limit voicemail server

Local or internal calling

Block long-distance or international calling

Safeguard infrastructure

Man-in-the-Middle (MitM) Attacks

- Intercepting and altering calls
- Stealing sensitive information,
- Changing the call content
- Both parties exchange communication
- Through the attacker's computer
- Active Directory Domain Services
- DNS configurations
- Redirect clients through their own server

Man-in-the-Middle (MitM) Attacks

Microsoft Teams

Prevent attacks on media traffic

Secure Real-Time Transport Protocol (SRTP)

Encrypts the media stream

Cryptographic keys are negotiated

Teams call signaling protocol

Highly secure TLS 1.2

AES-256 (in GCM mode)

Over UDP or TCP

Best Practices for Securing VoIP Systems

Best Practices to Secure VoIP Systems

VoIP engineer:

- Prepared beforehand
- Secure calls end to end
- Protected
- Malicious attacks
- Prioritize security and reliability

Encryption

Encrypt signaling and media

Secured protocol

Decrypted with correct key

Network Segmentation

Smaller and secure segments

Divide voice and data VLAN

Secure VoIP calls

Firewalls and Access Control Lists

Control access to network

Prevent unauthorized access to VoIP system

Session Border Controllers (SBC)

Protects network
placed at the border

Control access
defends against threats

Regular Security Audits and Updates

Conducting security audits

Install updates

Integration of VoIP with Other Communication Technologies

Video conferencing

- In conjunction with video conferencing
- Zoom, Teams, WebEx
- Participate in videoconferences
- Immersive and interactive experience
- Both audio and video in real-time
- Restricted travel during Covid-19
- Video conferencing a savior

Instant Messaging

Messaging platform

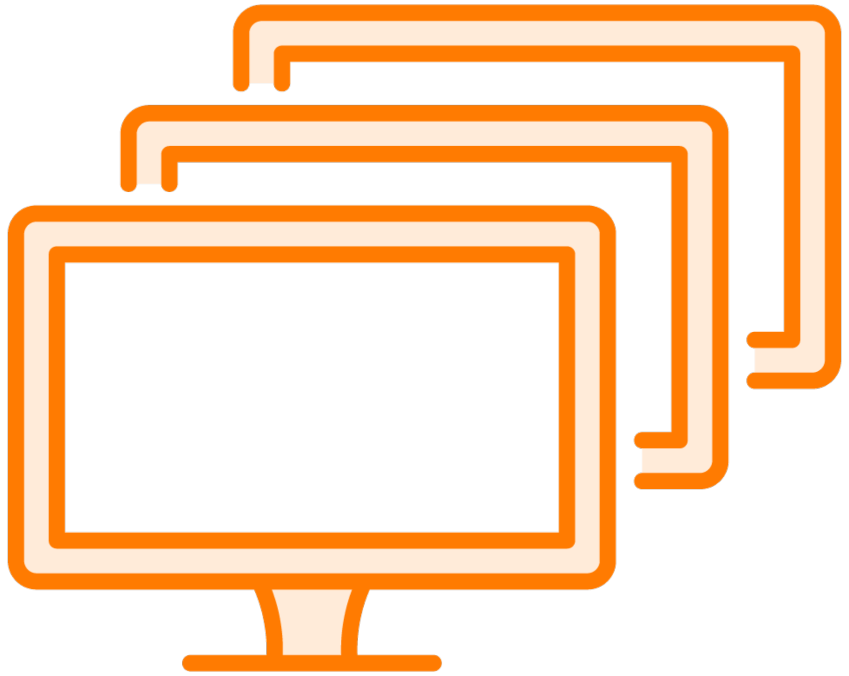
Slack or Microsoft Teams

Chat

Convenient communication

Switch between text, voice, and video

Screen Sharing



Used in:

- Presentations
- Demonstrations
- Remote collaboration

Applications:

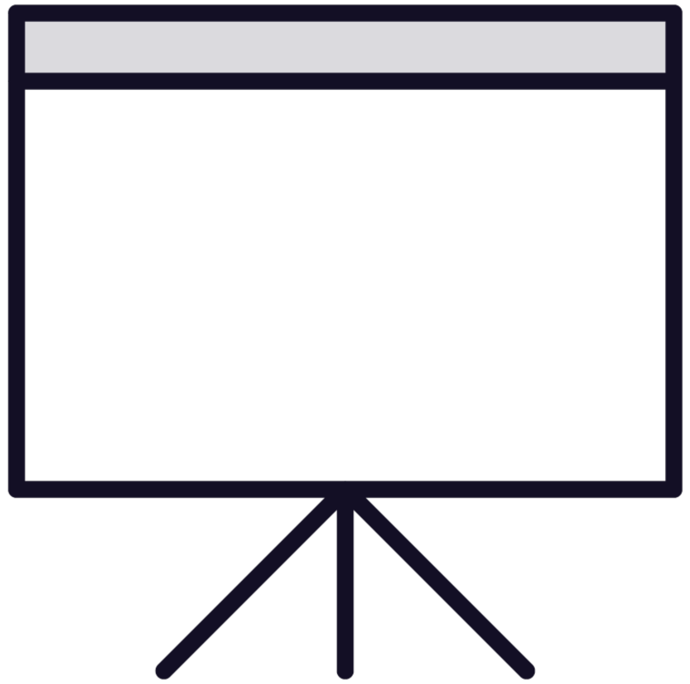
MS Teams, Cisco WebEx, Zoom

Engaging and interactive experience

View the presenter's screen in real-time

Questions or feedback

Whiteboard Sharing



- Real-time collaboration on a shared whiteboard
- Useful in educational or training scenarios
- Interactive and engaging experience
- Powerful
- Discuss and collaborate
- Located in different parts of the world

File Sharing

Platforms

OneDrive, Dropbox, or Google Drive

Share files and collaborate

Teamwork

In sync

Contact Centers

Handle customer calls and support inquiries

Customers contacts via multiple channels

Calls, email, chat, and social media

Unified customer interaction

Customer Relationship Management (CRM)

Seamless experience for customers and support agents

Access to customer information and interactions

Personalized user experience

Project Management

Asana, Trello, Basecamp

Collaborate effectively

Easy project management

Stay updated

Tasks delegation

Information sharing

Internet of Things (IoT)

Voice-activated smart devices

Control home devices using voice commands

Manage and monitor home

More Information

Artificial Intelligence Essentials: Smart Assistants

Navidut Tauhid

Emerging Trends and Technologies in VoIP

WebRTC

Revolution

Voice and video calls

- Browser
- No software installation
- Click to call

Cloud-based VoIP Services

Microsoft Teams, Cisco WebEx, or Zoom

Make and receive calls

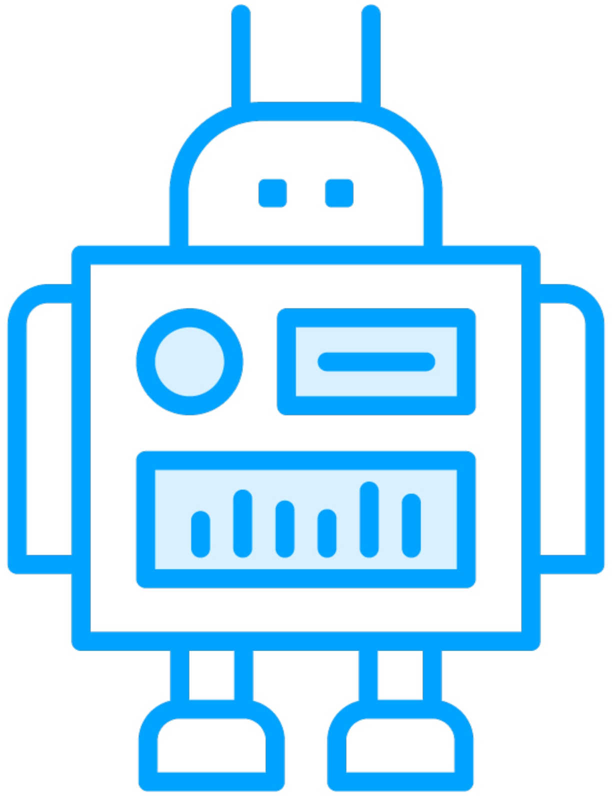
Alternate to traditional phone system

On-prem solution

Beneficial for

Small businesses

No upfront payment



Artificial Intelligence (AI) and Machine Learning (ML)

- Advanced call routing
- Voice recognition
- Speech-to-text conversion
- Virtual assistants
- Manage calls and meetings

5G Network

Faster and reliable

New possibilities for multimedia communications

Greater mobility

Voice Biometrics

Voice patterns to identify and authenticate users

Tight integration with VoIP system

Secure and convenient

Authenticate callers

Demo

Setting up and using a cloud-based VoIP service

Choosing the right solution:

- Requirements
- Budget
- Existing technology
- Support staff

Summary

Summary

- Common security threats
- How to mitigate them

Best practices for securing VoIP systems

- Encryption, access control

Integration of VoIP with other technologies