Whitepaper

Threat vectors in contact center

By Santosh Kumar,
Chief Security Architect,
Cisco Contact Center Business Unit

webex by CISCO

Contents

Introduction

When it comes to omnichannel cloud contact center, security and privacy becomes immensely important for the business. Before we dive into security and privacy aspects of the solution, it's important to understand the characteristics of the contact center business. Unlike any other cloud offers, contact center solutions deal with the most sensitive PII information. For instance, an end customer reaches out to the contact center using one or more of the channels and shares some of their sensitive personal information such as DOB, SSN, address, etc. for the verification process to an agent who is a complete stranger to the caller.

With digitalization on full roll, contact center is transformed from traditional voice into omnichannel by integrating various digital channels such as emails, chats, and social channel integrations e.g., Facebook and Twitter. Digital channels are growing at a phenomenal rate and it deals with the same level of sensitive data as traditional voice channel. The unique nature of omnichannel is that data is shared across all the channels, unlike multi-channel contact center. This makes security and privacy more challenging. In the next section, we will look at some of the threats and mitigation strategy.

Threat vectors and mitigation

In this section, we will dive into some of the key threat vectors and typical mitigation strategy that can be adapted for each of the above-mentioned channels. By no means, threats that are defined here is exhaustive but entail some of the key patterns that's been observed in the industry.

Voice

Voice is one of the long serving veteran of contact center world and still is used heavily as a preferred channel of communication within the contact center.

We will not discuss about the threats that are TDM/PSTN specific ones but a SIP and CPaaS (Communications Platform as a Service) based interconnection.

SIP trunking

SIP has become a defacto standard for any class 4 interconnect, cloud contact center would have to have some level of interconnection using SIP for inbound and outbound call routing. The following are some of the most common threats:

Trust worthiness

One of the primary threats with the Voice service provider not having a good operational hygiene. This could lead to serious confidentiality and integrity breaches. However, by having a robust security assessment process for vendors using CSA CCM matrix or similar to ensure that any third-party provider is deeply vetted before onboarding would greatly reduce this risk.

Network leaks

Lack of network segregation at Layer 3 would result in data leaks across tenant partition and any attacks that originates from Voice provider gets propagated into the core. One of the most common mitigation techniques is to maintain separate VRFs in addition to ALG and L3 Firewalls.

IVR and ASR attack vectors

IVR and ASR is most commonly used for automating routing of calls. Both IVR and ASR are prone to various attack vectors such as input validation attacks, SQL injection resulting from invalid input, fingerprinting, and internal data exfiltration when payment or sensitive information are logged. There are various mitigation techniques which can be adapted such as masking/ redacting of sensitive PII information, input validation, thorough testing of IVR/ASR menus and deploying WAF.

DoS/DDoS

DoS/DDoS are now a common attack vector for any VoIP trunks that are exposed. However, the good news is this can be easily prevented by deploying Session Border Controller and restricting each connection to a VRF level which would greatly reduce the risk.

Man-In-The-Middle Attack (MiTM)

MiTM can be used against SIP for performing attack vectors such as session hijacking and BYE attacks. One of the common ways to implement mitigation is to use TLS for SIP communication or implementing IPSEC which is slightly heavier than TLS implementation.

Lack of call encryption

The calls that are not encrypted are presented as RTP and it could be easily sniffed. In particular, contact center calls carry sensitive information so adequate measures must be taken. Thankfully, SRTP (Secured RTP) can be implemented as it makes use of AES 192 or 256 symmetric encryption (Only AES 256 is preferred). However, enabling SRTP alone is not good enough as the key exchange can be captured if the SIP traffic itself is not carried over TLS. Hence, in order to enable media encryption, SIP should be TLS enabled.

Data leaks in Call recording

In contact center, call recordings carry most sensitive PII information and any exfiltration of recordings would result in serious data breach. Most contact center solutions provide an option to agents for pause and resume of recordings. However, there is an element of chance due to human error that pause/resume feature are not always invoked. Even though PCI-DSS standard provides an option to have disk-based encryption with logical separation between tenants but it's not good enough for cloud native deployments. Hence why it is absolutely important that all call recordings are encrypted using tenant specific encryption keys (AES 256).

Communications platform as a service (CPaaS)

CPaaS is relatively a new kid in town for contact center integration but it comes up with a truck load of benefits such as deep application integration using APIs, elasticity, with built-in security and future proofing by supporting video channel with WebRTC. However, it shares most of the common threats with voice channels in addition to the below.

API key leaks

Most of the CPaaS provider uses custom keys for consuming their APIs. Any leak of those keys would result in confidentiality, integrity, and availability issues. In addition, general key management such as rotation of keys is not frequently performed and key strength/ crypto are not consistent across providers. Having such custom API keys would also result in vertical privilege escalation as most custom keys lack scope/entitlement checks. Therefore, its recommended that CPaaS providers support oAuth2 authorization framework. If oAuth2 is not supported then the contact center team need to have defined process for API keys rotation, storage in secure vaults and Cipher/key strength set to AES-256 as default.

Callback attacks

Unlike SIP trunk, some of the CPaaS provider uses webhook methodology to deliver notification of inbound calls or other call events. This presents new set of attack vectors such as unsolicited notification. There are good set of preventative measures that can be applied such as using shared secret to encrypt the payload, whitelisting CPaaS IP addresses and implementing mTLS.

Email

Besides voice, emails have been in a play for some time. However, it potentially carries significant risk when compared to voice. We will discuss some of the common threat vectors below.

Phishing

In general, phishing is considered one of the worst attack vectors due to human interaction. For the contact center, agent receiving one of those phishing emails could be really damaging. There are set of preventive measures that can be deployed such as ESA (email security appliance), DLP (Data Leak Prevention), AMP (Anti Malware Protection), more importantly agent training and regular testing of those controls for effectiveness.

Information disclosure

End-user and/or Agent could send sensitive data unintentionally without realization of the impact. This could result in data leak. One of the best mitigation techniques is to employ Data Leak Protection engine with default policies to scan and redact any sensitive information being sent or received by the agents.

Malicious attachments

This is probably the most common attack vector for enterprises. Its proven that 99% of these attacks are signature based so having a good AV and AMP at host and network level would reduce the attack vector significantly.

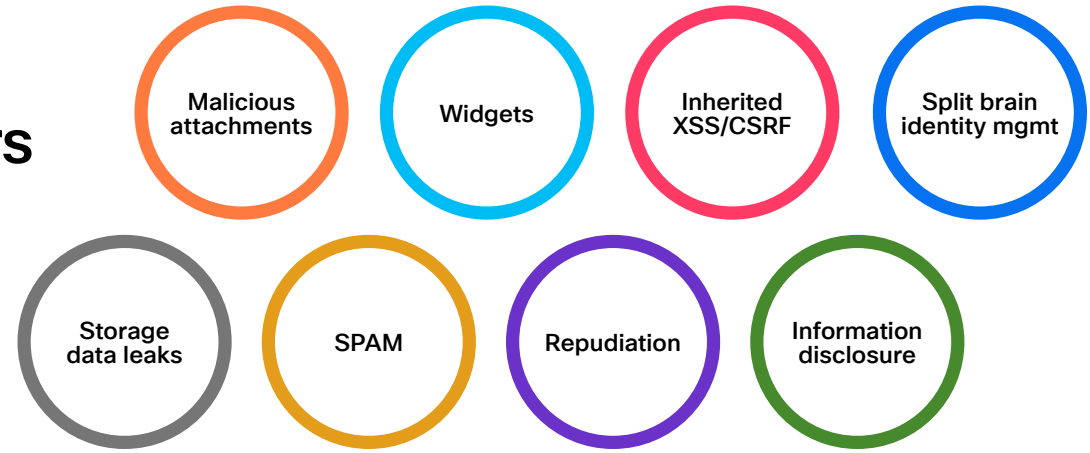
Repudiation

Repudiation is not one of the common attack vectors when compared with others. However, it can be equally damaging with financial consequences to the organization. Attack vector is when the user sends an email containing important financial or insurance related change and later denying performing the action. In order to mitigate this, system should perform non-repudiation by verifying digital signature of the sender.

Secondary Data leaks

This attack vector is very specific to omnichannel. When the system process emails for routing and if it's designed to store certain part of PII information for analytics or audit purposes without proper encryption then there is a high chance for date leaks via other part of agent interface. In omnichannel, unlike multichannel data travels through the message bus and chances of exposure of such data is significant. There are few ways to mitigate this such as email content should go through DLP engine before its processed and this way all sensitive information is redacted or masked. However, if the business need is to have those details stored not necessarily sensitive PIIs then tenant-based encryption can be applied.

Live chat threat vectors



Live chat

Chat is currently gaining a traction and is set to overtake email channel as it provides synchronous communication. In general, threat vectors to chat are more on the integration with enterprises web interface.

Widgets

Chat widgets contains many attack vectors particularly if the origin is not known or if it's an OEM solution. One of the serious attack vectors is the persistent XSS in chat widgets. There are various mitigation techniques that can be applied such as input validation, output encoding, implementing a proper CSP and apply integrity checks using https://www.w3.org/TR/SRI/.

Inherited XSS/CSRF

If the widget is integrated into an enterprises insecure Web interface which is prone to XSS or CSRF then the chance of attack propagation into the widget is high. In order to mitigate, enterprises web interface should be vetted before the widget is introduced and WAF should be included in the path.

Split brain identity management

The attack vector i.e., the end-user logs into enterprises web interface using a different identity provider than the one used by the widget. Widget then uses built-in/pre-set oAuth token or equivalent to communicate with the contact center backend. Attacker could get hold of the token that's exposed for the widget and perform another form of attack against contact center backend. The primary problem here is different auth framework is used between widget and the web interface. The mitigation for this is straight forward, Web interface / Widget should integrate with the same identity provider and use the token that belongs to the user not the default or service tokens.

Information disclosure

This attack vector is same as the one in Email channel and therefore a similar mitigation technique can be applied.

Repudiation

It's also same attack vector defined in the email. However, abuse case and mitigation technique are different because there is no digital signature in play. In the chat, business requirement could be to allow guest login access without needing to register. The mitigation should be guest access should have restricted functionality and never be allowed to escalate into registered user without relogging with a different session ID to avoid any session fixation attacks.

Storage data leaks

This is similar to Secondary Data leak vector in email channel. The same mitigation techniques can be used.

SPAM

It's the most prevalent threat vector for the chat that allows guest logins. In order to mitigate, various filters can be added such as CAPTCHA/reCAPTCHA, time-based checks and other commercial antispam specialized for chats.

Malicious attachments

This is exactly the same vector mentioned in the email. However, the critical aspect is that the chat is synchronous so scanning should happen instantly before its forwarded on to agents. To avoid overload on the scanning, only specific types of attachments should be allowed with size restriction.

Social channel

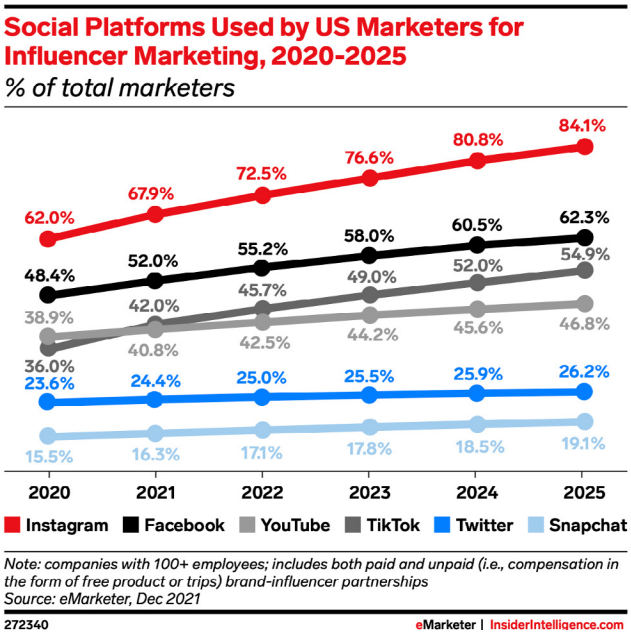
Social channel is evolving to be the most preferred channel of communication and its quickly making a way into the contact center (as reflected above in the picture). Social channels inherit all the threats that are in chat, in addition it brings in following overheads to consider.

Token management

In general, social channel integration is done based on oAuth grant flow. This means that the contact center solution must deal with end-user access and refresh tokens. It's important that such tokens are managed using vault and accessed via tenant's key.

Privacy and Legal impact

Before rolling out any design discussions It is important to understand privacy and legal terms for integrating with social channel. For example, Facebook and Twitter have specifically called out conditions on third party integrations.



Security baseline

This section will address some of the baseline security requirements that are required for cloud-based contact center solutions.

Data touchpoint

Broadly speaking, an omnichannel contact center is data rich and goes through various touchpoints such as:

- Agent and customer interactions
- Used for gathering analytics
- Workflow Management/Optimization requirement
- API's for integration
- Maintaining recordings for legal/regulatory reasons
- CRM integration on the agent side

One of the key elements of cloud contact center is to store minimal amount of personal information in the nonvolatile storage (NVS). In fact, only complaint/regulatory-related information should be stored and the rest of them should be collected/processed via integration with enterprises CRM. The data that is stored in NVS should be encrypted using tenant-based encryption and PII data that are used for the processing should be redacted or masked where possible. The PII data in volatile storage such as message queues(redis/kafka) should be encrypted using tenant-based encryption key if masking/redaction is not possible.

Identify and Access Management (IAM)

Cloud contact center should have SSO enabled by default for dealing with agent/user identity. In addition, federation via SAML2 should be provided as an option to the enterprises.

Authorization

Authorization primarily deals with access management. It's one of the important aspects of RBAC (Role Based Access Control). The OAuth2.0 authorization framework should be supported by API's and other contact center integration. API's should have enforcement based on scopes, roles, and entitlements.

Encryption

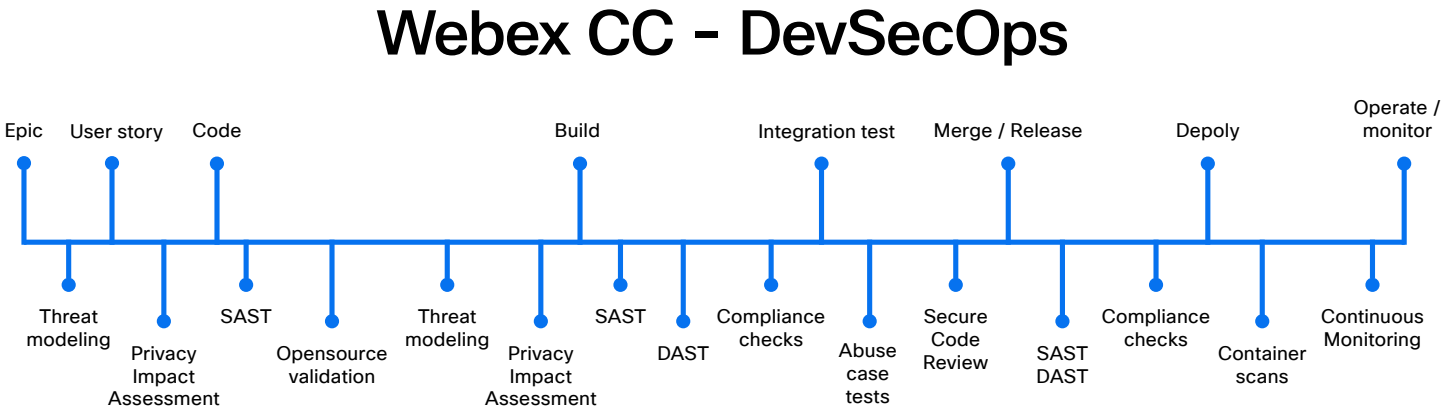
Encryption should be supported at both Transit and at rest. In addition, where possible end-end encryption should be applied. It is recommended to implement FIPS 140-3 for encryption.

AI

AI is becoming integral part of the contact center as it offers value added services such as Natural Language Processing (NLP), Agent Assistant and Virtual agents. AI use cases for the contact centers translate broadly into NLP, Machine Learning (ML) and Deep Learning (DL). In order for NLP and ML/DL to deliver best results, it needs reliable training data which has to be close to the user generated content. However, supplying such data would break the security, privacy, and legal stature. This article captures details about some of the ML security posture. You can also check out this article on how to identify six new risks of AI and how to combat them.

DevSecOps

In order to maintain consistent security posture, it's important to get some of the security tenets right into the CI/CD process. The above picture depicts Webex Contact Center's DevSecOps program – each of those milestones has security gating process so that necessary metrics are collected. It's critical to have



Summary

The threat vectors discussed in this white paper only provides some of the common patterns that occurs in the contact center. By implementing security and privacy controls at both channel and baseline level it will most certainly improve the security posture.

In Webex Contact Center, we have addressed these threats at platform and application level. But most importantly, our DevSecOps have these fundamentals built into the scrum cycle.

For more information
Please visit the Webex Contact Center page

March 2026