Akkadian Labs®

WHITE PAPER

Enhancing Security and Mitigating Risk for Cisco Collaboration Technologies

Best Practices for Risk Mitigation in UC

By Tom Bamert, *Chief Technology Officer, Akkadian Labs*
March 2019

EXECUTIVE SUMMARY

Cyber security should be a high priority for users of Cisco Unified Communications technologies. While CUCM, Unity Connection, Webex, Jabber and related collaboration software may not seem like attractive targets for hackers, such systems expose organizations to several operational cyber risks (i.e. risks associated with procedures rather than inherent in the software itself). This is particularly true as other areas of IT, such as networks and databases, get better protected. Attackers are now seeking to penetrate businesses through any exposed surface area, including unified communications (UC).

This paper looks at ways to mitigate risks in UC. It examines how InfoSec policy can expand to include collaboration, which has not usually been considered in an entity's overall security posture.

Findings include:

1. Unified communications systems expose your organization to operational cyber risks
2. Costs of UC fraud, spoofing, service disruption, eavesdropping and more now exceed $29 billion a year
3. Mitigating UC security risks can be accomplished by
   - Limiting access to the native UC products
   - Implementing role-based administrative privileges
   - Tracking user activity
   - Minimizing errors with a "single pane of glass"
4. **Akkadian Provisioning Manager** is an enterprise grade solution which enables you to easily operationalize each of these countermeasures to the risks

INTRODUCTION

Unified communications technologies may seem to be outside the purview of cyber security, but UC is part of your exposed attack surface area. As cyber attacks grow more sophisticated and core IT systems become better defended, hackers are looking for any vulnerability they can exploit. Risks from a compromised UC system do exist, especially those involving social engineering. This white paper offers a solution by providing a way to mitigate risks in UC using commercially available software.

SECURITY RISKS IN UC

Unified communications systems expose your organization to cyber risks. The risks may not be glamorous or high-tech, but they can still have an impact on your security vulnerability. One issue is that many cyber-attacks and frauds start well outside of the systems that are the ultimate targets of the attack. A criminal may want to defraud your company by penetrating your financial systems. However, the way in might involve social engineering rather than the picking of digital locks. In social engineering, hackers impersonate coworkers, bank employees, suppliers and so forth.

A compromised UC platform is a fertile ground for this kind of mischief. It's a major problem. Research by the Communications Fraud Control Association (CFCA) estimates that telecom fraud costs organizations and carriers over $29 billion year.

Unauthorized access to UC back end

The relative isolation of UC exposes the system to risk. On its own, UC is vulnerable to unmonitored back end tampering. UC access is controlled, of course. Many companies use LDAP (e.g. Microsoft Active Directory) to authenticate UC users. The problem, however, is with authorization. Granular control over authorization is much harder to realize in UC.

A malicious actor with unauthorized access to the UC back end can set up, modify or delete accounts. This enables the hacker to impersonate users or take advantage of access to learn details about the business that he or she can use to commit fraud.

Alternatively, a legitimate but inadequately trained admin might accidentally create security problems. For example, if an employee leaves the company, it's customary to terminate all UC access. However, if the admin does not know how to do this properly, working on the complex UC back end, you could end up with a former employee who retains access to one or more UC applications.

The basic vulnerability rests with the nature of the UC back end. In its native form, it lacks granularity in security control over the individual applications. In the wrong hands (either inexperienced or malicious), you could have substantial risk exposure.

Spoofing, fraud and eavesdropping

Access to a UC account gives a malicious actor a multi-faceted toolset. By spoofing a legitimate-looking phone number, for example, a hacker could call people and pose as an employee of your company. They could disrupt or embarrass your business in this way.

Or, they could eavesdrop on internal conversations. There are many risks in this scenario. In particular, the hacker could gain access to proprietary information for use in insider trading or "hacktivist" schemes to make your company look bad. Rerouting of calls to outside numbers similarly exposes your organization to risk.

The main risk, though, is of fraud. When a malicious actor can credibly pose as an insider, especially as an executive, he or she is able to steal from your business. For example, a hacker impersonating a senior executive could request a wire transfer to a bank in payment for services to a fictitious vendor. This is known as a "CEO fraud" or "command fraud" and unfortunately, it's quite common. If an employee gets a call from the "CEO"—or someone who has the CEO's extension number in the office—he or she is likely to follow whatever instructions are given.

Misuse of UC credentials to penetrate networks and other IT assets

An attacker can use unauthorized access to a UC account to breach critical systems. For instance, by posing as a member of the IT staff, the hacker could request login credentials for enterprise applications. Then, with those credentials, he or she could breach the system without raising any alerts. After all, it would look as if an authorized user was conducting a legitimate session.

Accidental or deliberate service disruption

Service disruption is another risk of unauthorized or untrained UC back end access. Availability of systems is a pillar of information security. If UC is not available, that will have a detrimental impact on the business. Even if it's by accident, it's still a security problem. Shutting down UC is a good way to make life miserable and unproductive for your company.

MITIGATING SECURITY RISKS IN UC

> If you have never been involved in responding to a cyber security incident, you may not think it matters much that an IT person can get back end access to UC without control over authorization or any centralized record of his or her session. If there is a cyber incident, the first things you want to know are "Who did what, when?" For example, a data breach could occur because someone improperly patched a server. It could be a simple mistake, but if the security operations (SecOps) team doesn't know what happened, their response will be delayed and ineffective.
>
> To mitigate this risk, most security teams carefully monitor assignments of administrative privileges. There's even a sub-specialty of security known as Privileged Access Management (PAM) to track administrative access. It's a good practice to restrict administrative access to a select group of people.

Avoid granting direct access to native UC products

One simple countermeasure is to avoid granting direct access into native UC apps for IT department or HelpDesk users. It is tempting, given the pressures we all face on budgets and personnel, to let lower level or outsourced IT people deal directly with provisioning and account management for the Cisco collaboration suite. This is a mistake, considering the complexity of the UC back end and its security risks. Given that unmitigated access to the back ends of native UC apps introduces risk, it's a good security practice to restrict access to a few, trusted people.

Akkadian Provisioning Manager is a software layer that sits between users and the native Cisco UC products, which offers trackable, managed UC admin. It simplifies the work of provisioning and managing accounts for multiple Cisco UC applications.

Assign privileges by role

One effective way to restrict risky, overly broad administrative access to UC is to implement role-based administrative privileges. Each admin role can be different. One type of admin might be able to provision accounts in groups, but not delete accounts. Another might be able provision and delete accounts on one application, but not another, and so forth. Granularity in role-based admins offers a higher level of control than unfettered access to making updates to the UC.

Akkadian Provisioning Manager enables this capability. In this mode of operating, not everyone has equal abilities to provision or modify UC accounts. In fact, the best practice is to limit "super admin" rights to perhaps just one individual. The super admin can do everything, including setting up other admin roles.

Tracking user activity

Finally, as we noted earlier, it is important for security to be able to identify "Who did what, when?" The native Cisco Collaboration product suite has limited ability to track user activity.

Akkadian Provisioning Manager gives you full, highly granular user activity tracking so you can always go back and determine the source of any change that might have been the cause of a negative impact on your UC environment.

Minimize errors with a "single pane of glass"

Errors when implementing moves, adds, changes and deletes (MACDs) can open gaps for exploitation by hackers. For example, if an employee leaves the company and is de-provisioned from voice calling but not from instant messenger, that is a point of vulnerability.

Akkadian Provisioning Manager provides a unified interface, a single "pane of glass," so to speak, for automated provisioning across multiple UC servers and applications. This reduces the potential for MACD mistakes.

CONCLUSION: BRIDGING SECURITY POLICY AND UC

> Using a solution like Akkadian Provisioning Manager to implement controls over UC administration is a worthwhile step to take to improve your organization's security posture. It should be part of a larger thought process, however. UC should firmly occupy a place in your overall security policy framework. If it isn't, that's a deficiency that you should remediate. The growing seriousness of cyber threats and the tendency of attackers to seek less-guarded points of entry make the issue even more relevant today.

Akkadian Labs®

ABOUT US

Collaboration, an increasingly fundamental characteristic of successful businesses, is often overlooked. Creating software that helps people collaborate is our focus. We offer software products and solutions that integrate Unified Communications environments as well as other business focused enterprise applications.

Technology is complex.
We make it simple.

Want to learn more?

Schedule a Demo

Contact Us

Contact Us to Learn More About Our Software Products
sales@akkadianlabs.com | **www.akkadianlabs.com** | **1-800-818-4128**