TOLL FRAUD

HIGHLIGHTING THE NEED TO SECURE ENTERPRISES COMMUNICATION SYSTEMS

APPLICATION NOTE

Alcatel·Lucent Enterprise

TABLE OF CONTENTS

INTRODUCTION

Fraud against telecom service providers, operators, subscribers and enterprises is increasing. This growth is motivated by the ability of fraudsters to make money by exploiting the absence of an effective international telecommunications regulatory authority or enforcement mechanisms, combined with gaps in organizational security for telecommunications systems.

CUSTOMER SCENARIOS

1. A company's IT manager discovers a spike in international long-distance calls to a country they're not doing business with – outside of regular office hours.
2. The monthly accounting report of another company shows a significant volume of calls placed to international numbers – from the same internal phone.
3. A store with 20 employees receives a monthly phone bill equivalent to its past 3 years' bills combined.
4. An organization receives a fraud alert from their telephone operator – at the same time as they detect multiple, regular, short-duration calls to a premium-rate number.

Fraud losses are up 15.4% since 2011

WHAT HAPPENED?

These scenarios are examples of customers experiencing toll fraud. All organizations, from small offices to multinational companies are potential victims, regardless of their communication system vendor. And the number of attacks is rapidly increasing.

Toll fraud is the unauthorized use of a communication service by an unknown third party. It can involve scammers reselling call minutes to long distance numbers through an unsuspected entity (such as a compromised PBX). Another example is premium-rate service fraud, in which a communication system or service is exploited to place calls to special international services numbers that levy a per-minute or per-call charge on the subscriber.

Fraud can cause tremendous financial losses before they are detected – in the worst case, a full month can pass before the account report is received and the fraud identified. Fraud can even damage the brand reputation: there have been cases reported in which customers calling their personal advisor are instead connected to an unrelated – and potentially embarrassing – premium rate service. Moreover, by overloading the communication server resources, such frauds may impact telephony services availability, potentially leading to a complete loss of service.

Estimated Fraud losses from PBX hacking in 2013:

$4.4 billion (USD)*

Why is telecoms fraud expanding?

The rise of social networks and social media have made it extremely easy to create and distribute cookbooks – short videos and tutorials that explain how to compromise communication systems. Very little telecommunication skills are needed to access unauthorized services and make money from communications that take advantage of a targeted company's resources.

In addition, while protection mechanisms are embedded in communication systems, vendor security recommendations are often not fully implemented and configurations are not optimized due to a lack of awareness. These security oversights can facilitate hacking.

Finally, companies with aging systems are potentially more exposed to these types of threats.

How do fraudsters operate?

Typically, fraudsters gain unauthorized access to a communications system from outside the company through security breaches. Past methods involved hacking into the PBX directly through the maintenance port, but techniques have evolved and now include diverting voice applications, and tricking end-users therefore making it difficult to trace and detect callers as the call appears to originate from a "trusted entity" instead of the fraudster.

The most popular methods include:

Remote maintenance

Hackers detect the modem attached to the maintenance port and try to log in using the default password, which administrators often fail to change. Once in the system, hackers are free to change the configuration as well as logins and passwords.

Voice mail

This method targets voice mail, which is hacked by exploiting poor password control. Typically, the attack aims at using the voice mail system to make outbound calls to a premium-rate or long-distance number. Teleconference bridges with multiple-line conferencing capabilities make prime targets.

Call barring

In addition to poor password policy, hackers can also benefit from lax call controls, which provide safe conduct for their war dialer software to place unlimited calls to premium-rate or long distance numbers.

Direct Inward System Access (DISA)

This service, designed for remote workers, allows employees to access internal telephone services from remote locations. Full or partial PBX functionality can be exploited remotely by malicious users if the DISA service is insufficiently protected (e.g., single access code, no caller ID control).

External transfer, external forwarding

External phone feature rights – if not appropriately set – provide hackers the ability to easily develop fraud scenarios. Some exploits, however, require an accomplice within the company.

WHAT MOTIVATES FRAUDSTERS?

While toll fraud can be used to harm a company's financial health or to damage a competitor's reputation, it is most frequently used for financial gain. Alcatel-Lucent has seen examples in which fraudsters make $20,000 (USD) in four hours – fast and easy money. Fraudsters can also be present inside the company, such as dishonest employees who are attracted by the prospect of diverting company resources for personal gain.

The number one emerging fraud method is PBX hacking*

ASSESSING ORGANIZATIONAL VULNERABILITY

Have the same system passwords been used for more than a year?

Do end-users use default voicemail password?

Are modems connected to the communication server?

Are all end users granted access to international numbers?

Are telephone services provided to users outside the company?

Has the system administration team recently undergone personnel changes?

ANSWERING "YES" TO ANY OF THESE QUESTIONS REVEALS POTENTIAL RISK.

PROTECTING COMMUNICATION SYSTEMS

Applying Alcatel-Lucent protection mechanisms and best practices to communication systems helps optimize both configuration and security, and avoid many toll fraud scenarios.

Take appropriate security measures

- Call barring: restrict outbound calling during non-business hours, require passwords for long-distance calls and forbid calling premium-rate numbers.
- Review password policies: change default system passwords, and continue to change them on a regular basis (e.g., monthly).
- Implement external transfer and forwarding protection.
- Review responsibilities and administration rights.
- Update system database by removing former end-users' information.

Reinforce internal awareness

- Educate employees about elementary security practices and related impacts (e.g., legal and financial risks), and about their duties and responsibilities.
- Remind workers about common-sense practices regarding confidentiality rules, such as never disclosing technical details about information and communication systems to unknown callers (e.g., personal codes, names, IVR and voicemail services direct numbers).
- Develop fraud awareness campaigns: encourage employees to report unusual behavior or activity on telephony services, including strange messages on voice mailboxes, busy lines early in the morning, and call logs reporting several calls during non-business hours.

Leverage the expertise of your Business Partner and Alcatel-Lucent

- Keep software releases up-to-date to benefit from the latest product enhancements and technology evolutions.
- Strengthen solutions by implementing security best practices.
- Apply the latest vendor security patches.
- Regularly assess the communication system's exposure to toll and premium-rate number frauds.

* Source: Communications Fraud Control Association, 2013 survey

Alcatel·Lucent Enterprise