Concept Note

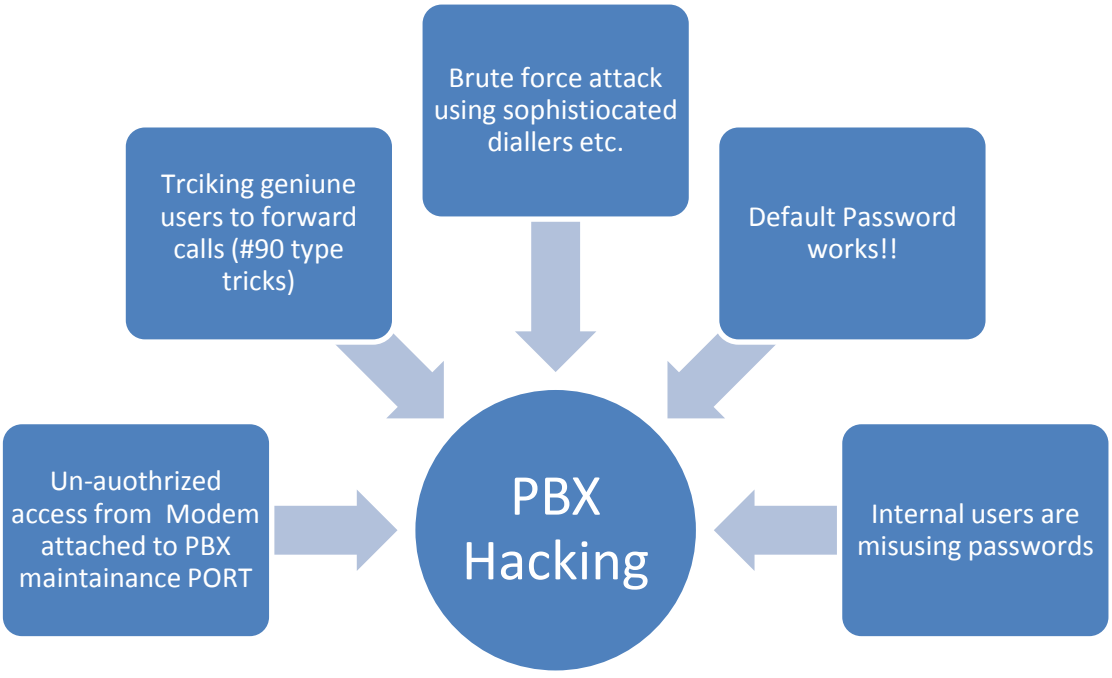
PBX Hacking

Concept Note on PBX Hacking

A PABX/PBX (Private (Automatic) Branch eXchange) is telephone equipment that is installed on corporate premises to provide a number of telephone extensions within an office and operate as a connection between the business and the external dial-out network. A PBX allows sharing of outside lines and thus significantly reduces the number of such lines needed to be leased from a Telco. PBXs have evolved over time in much the same way that Telcos have evolved, moving from circuit switched to IP-based packet technologies. An on-site PBX provides more telecommunications service control to the organization. Today, even the most basic PBX systems have a wide range of capabilities that were previously only available in advanced large-scale switches. Today's voicemail platforms often have similar capabilities to PBXs, and thus are prone to similar attacks.

Typically, incidents tend to occur when business premises are unattended, PBX use is not monitored, and/or the PBX is accessible externally. Calls are placed and routed via the PBX and, in the majority of cases; the business owners are unaware of the event. In the most extreme cases, losses of thousands of Dollars can be incurred by businesses due to this type of fraud. We should understand that these "attacks" are possible because the victims are largely unaware of the potential threats and the PBXs in question have not been properly secured.

Popular methods of hacking PBXs are summarized in diagram below.



Brute Force Attacks: Typically, the PBX security is breached via the toll-free Direct Inward System Access (DISA) number. Many PBXs allow dial-through, wherein a person calling into the PBX can access an external line by using appropriate passwords and control sequences. Large corporates use this feature extensively. Fraudsters hack into the PBX, obtain passwords and once a password is retrieved, use the PBX to generate outbound calls (typically for call selling or PRS revenue share).

"War dialing" is one of the techniques used for obtaining passwords. It involves the fraudster trying to break PBX code using an auto dialer, which keeps on dialing same number in a sequence making an exhaustive search of passwords until it breaks through.

Default Passwords: One of the largest contributing factors in PBX hacking and misuse is careless PBX installation and poor configuration, leaving default user and maintenance port passwords in place (fraudsters know the default passwords for the various switch vendors). PBX fraud commonly occurs when the customer fails to change the default password or do not change passwords frequently. Default passwords can be found online in the relevant PBX user manuals etc. Telco and PBX vendors should advise corporate customers to changes all default settings and passwords. This will prevent easy hacking opportunities for fraudsters.

Internal Enemy: Many cases of PBX hacking result from insiders or vendors who disclose the phone numbers, IDs and passwords necessary for breaching PBX security. Sometimes the users may get hold of passwords by unauthorised means and use the corporate lines for making personal calls or colluding with external fraudsters to help in PBX hacking. Strict security Policies should be in force for PBX password control. The physical security of PBXs and phone extensions is also an important factor to consider in avoiding misuse of PBXs.

Social Engineering: The old traditional (wired) phone scam involving the 90# buttons on corporate telephone lines is still around. Employees of a corporation using a PBX line from their desk, receives a call from someone claiming to be a telephone company employee investigating technical problems with line, or checking up on calls supposedly placed to premium rate services or other countries from your line. The caller asks the employee to aid the investigation by either dialing 90# (or similar combination) or transferring him/her to an outside line before then hanging up the telephone receiver. By doing this the employee will be enabling the caller to place calls that are billed to the corporate telephone account. This attack only works on few PBXs today. Social engineering is another common technique used for obtaining passwords.

Service Port: PBX hackers may also target modems attached to the service PORT of a PBX. The facility is provided by PBX manufacturers to allow remote support of the PBX. Typically, the connection should be opened only when an authorized request goes from the PBX customer to the PBX vendor, but many PBX customers keep the connection always open and therefore prone to attack.

In addition to theft of service, the following misuse can occur through PBX hacking:

- **Disclosure of Information** such as eavesdropping on conversations, or gaining unauthorized access to routing and address data.
- **Modifying Data** such as change billing information, or modify system tables to gain access to additional services.
- **Denial of Service attacks** such as changing passwords to deny access, or forcing PBX to fail or degrading quality through excessive calling volume.
- **Traffic Analysis** such as observing information about calls and make inferences (industrial espionage), e.g. from the source and destination numbers, or frequency and length of calls.

Preventive Actions

Telco Customer:

- Should be informed of potential security threats to the PBX;
- Should maintain and enforce good security policies for the PBX;

- Should educate employees about threats (especially social engineering related) used for PBX hacking;
- Should ensure physical security of the PBX, phone lines and other equipment;
- Should Monitor international calls and high value services use through the PBX.

Telco Protection through the FMS:

Simply by monitoring high usage for types of calls or traffic not expected for corporate customers. PRS calls, content download, and international calls to high-risk countries during unusual hours (e.g. night or weekend) can be good indicators that a company's PBX has been penetrated. Since many companies don't closely monitor their detailed phone bills on a line-by-line basis, this can otherwise go unnoticed for long periods of time.

FMS rules should be configured for off peak monitoring with appropriate filters and thresholds, high usage monitoring for PRS, content and International services, hotlist rules for high risk country codes and equipment identifiers. It is advised that xDRs (Usage record) processed in the FMS should have a field indicating whether a call originated or terminated at PBX.

Once PBX hacking is detected, similar compromised lines can be identified based on behavioral profiles of blacklisted subscribers.

Authorization failures from PBX (or Voicemail) authentication can be monitored using rules on log files.

The FMS should allow the users to define behavioral patterns, which are to be monitored and combine events (rules) logically (using Boolean operators) to define specific behavioural patterns. An example of such a pattern is large number of short duration incoming calls followed by outbound international calls.

Profiling can be used to spot sudden changes in volume and/or the nature of use of PBXs. Again this is a strong indicator that a PBX has been hacked.

Further Reading:

http://www.infosecurity-magazine.com/view/2182/pbx-hacking-moves-into-the-professional-domain-as-arrests-stack-up-/
http://www.experts-exchange.com/articles/Other/Miscellaneous/Phone-PBX-Hacking-Prevention-Tips.html

About Subex Limited

Subex Limited is a leading global provider of Operations and Business Support Systems (BSS/OSS) that empowers communications service providers to achieve competitive advantage and deliver new service experiences to subscribers. The company pioneered the strategic concept of the Revenue Operations Center (ROC) – a centralized framework for end-to-end control of a service provider's revenue and costs, fostering operational dexterity for sustained profitability. Subex's software portfolio powers the ROC and its best-in-class solutions enable new service creation, operational transformation, subscriber-centric fulfillment, provisioning automation, revenue assurance, cost management, data integrity management, fraud management and interconnect/interparty settlement.

Subex's customers include 36 of the world's 72 largest service providers. The company has more than 300 installations across 70 countries.

For more information please visit www.subexworld.com

www.subexworld.com

Subex Limited

Adarsh Tech Park, Outer Ring Road,
Devarabisanahalli,
Bangalore - 560037
India

Phone: +91 80 6659 8700
Fax: +91 80 6696 3333

Subex Inc.

10385, Westmoor Drive,
Suite 210,
Westminster, CO 80021
USA

Phone: +1 303 301 6200
Fax: +1 303 301 6201

Subex (UK) Ltd.

3rd Floor, Finsbury Tower,
103-105 Bunhill Row,
London, EC1Y 8LZ
UK

Phone: +44 20 7826 5420
Fax : +44 20 7826 5437

Subex Americas Inc.

30, Fulton Way,
Richmond Hill, Ontario,
Canada L4B 1E6

Phone: +1 905 886 7818
Fax: +1 905 886 9076

Subex (Asia Pacific) Pte. Ltd.

175A, Bencoolen Street,
#08-03, Burlington Square,
Singapore 189650

Phone: +65 6338 1218
Fax: +65 6338 1216