VOICEMAIL PROTECTION

INVISIBLE

SIMPLE

TRANSPARENT

Auto protection system for on-server voicemail/voice memo systems
Demonstration by arrangement

PROBLEM

Voicemail hacking and unauthorised access is very simple in most cases and very prevelant.

Customer actions required to prevent unauthorised access are not being taken.

Current voicemail "protection" is a simple 4-digit "lock" on the message box. Once "in", the hacker has complete access to all messages.

There is no evidence of intrusion

Campbell Scott
Telecoms Consultant

"Voicemail is a very important tool for mobile network operators in maximizing the proportion of calls attempts that are completed within the network. This results in very significant call revenues, due to; an increased number of completed calls, from the resulting calls to retrieve messages and from returned calls. This means that a significant portion of a mobile operator's call revenues directly result from voicemail capability. Mobile Operators are therefore concerned about the risks that have been highlighted by the press coverage and will take actions to ensure that customers retain confidence in the security of their voicemail box. From initial testing of the proposition, I have confirmation from both O2 Ireland and Meteor/eMobile, that they are exploring options to improve voicemail security and to provide customers with assurances as to the security of voicemail and the protection of their privacy."

Barbara Dixon
US Senator

Sen. Barbara Boxer is urging that telecommunications companies Sprint Nextel and T-Mobile improve voicemail security in light of the ongoing U.K. scandal accusing Rupert Murdoch's media empire of phone hacking.
"Right now, the voicemail accounts of Sprint customers are at risk of being hacked because of your company's security policies," Boxer wrote in her letter to Sprint CEO Dan Hesse.
"We strongly encourage the customer to continue using the passcode," Sprint said in its statement. "If the customer chooses to skip the passcode, they are warned with strong language that the voicemail account will be vulnerable to unauthorized access."

VOICEMAIL PROTECTION

Caller

INVISIBLE SIMPLE TRANSPARENT

SOLUTION

Prevent unauthorised access to actual individual voicemail messages (not just to prevent access to the mailbox, as per normal practise). This means that the voicemails are protected even if an attacker or malicious employee did manage to access the mailbox or if the servers / hard drives on which they are stored were accessed or stolen.

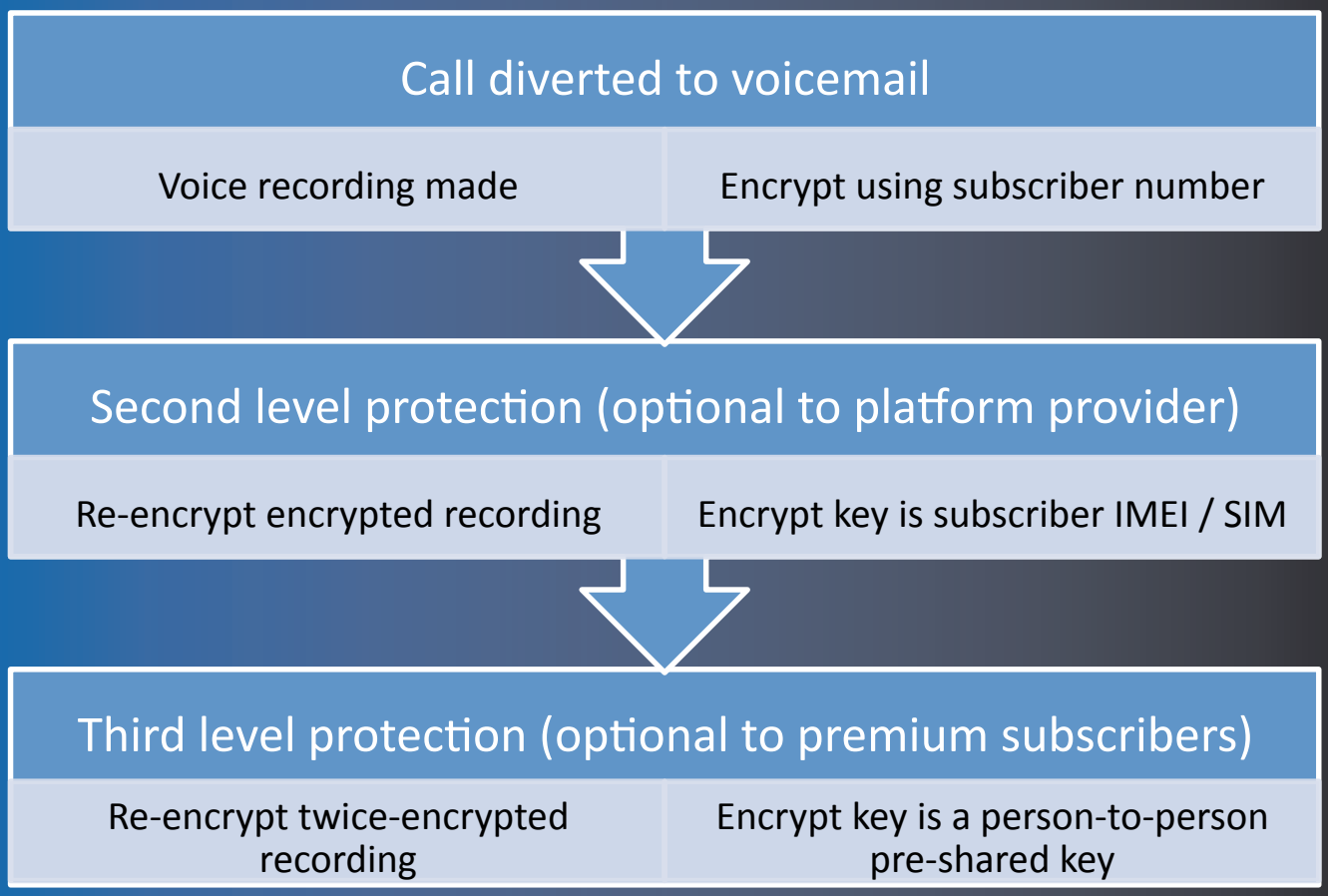
The solution is not only fast and efficient but is completely transparent to the end user and will integrate with minimal configuration into industry platforms.

The system also offers hyper-protection on a 'per-relationship' basis for users who are very security conscious. Single-use randomised protection is also possible.

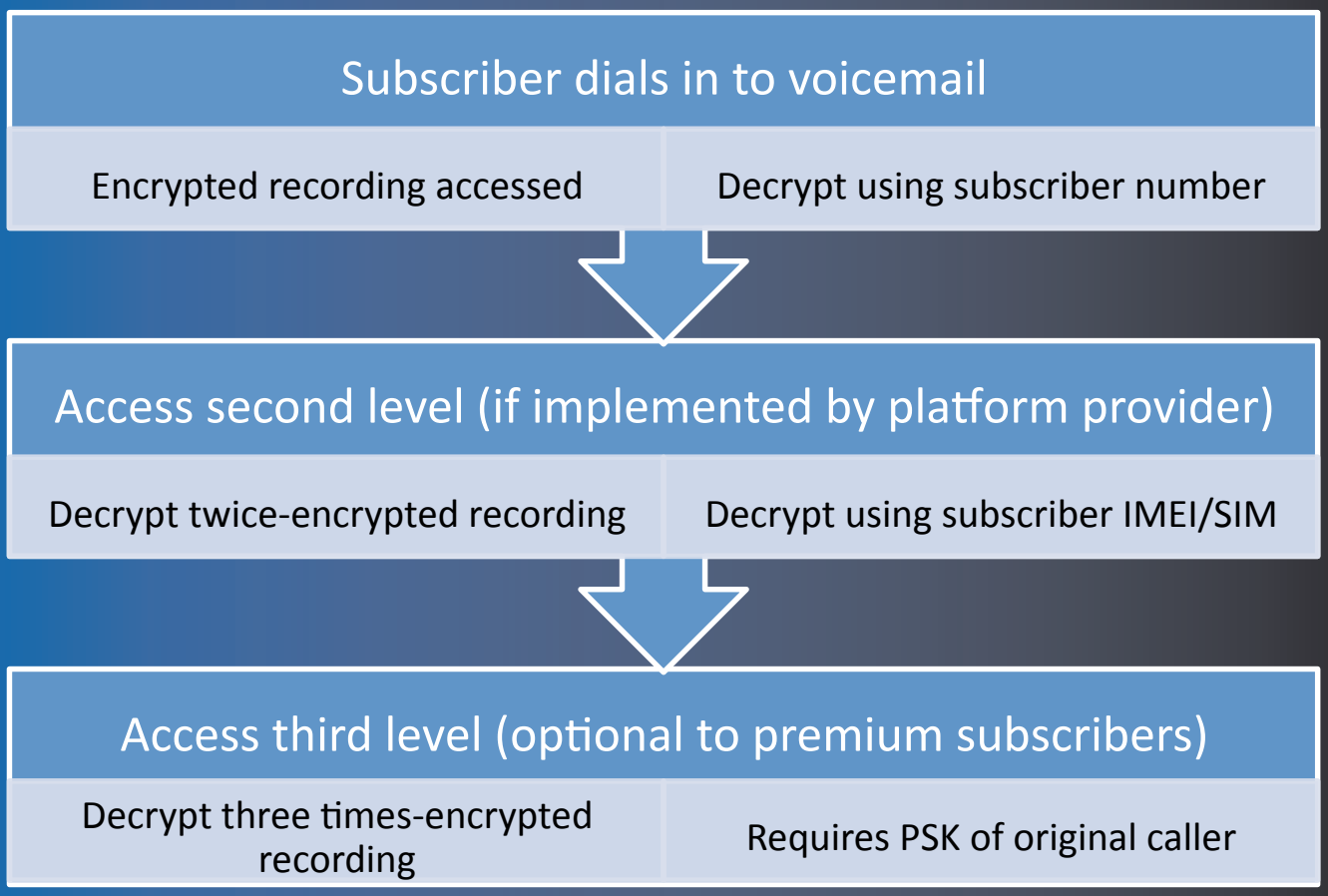
A unique feature of our solution is the ability to automatically identify and flag any attempted attack, before then locating, identifying and reporting the attacker identity and (if required) sending an alert to both the hacker and the innocent victim to notify both of the detection.

Features:

- All messages are protected automatically.
- No end-user action required by caller/recipient.
- No Apps required. No software upgrade required.
- Backward-compatble.
- Immediately accessible to ALL handsets, including on calls originating from 'landlines'.
- All encrypting and decrypting automatic on TelCo server
- Protection can be double-layered using subscriber number & most recent IMEI/IMSI if required, thereby preventing 'hoax' or 'cloned SIM card' access.
- NB: Although IMEI/IMSI details are not transmitted in-call, so they cannot be intercepted on the fly, the system is designed to allow TelCos to use internal/private identifiers instead if required.



VOICEMAIL PROTECTION FLOW CHART



digitalWEED.ie
info@digitalweed.ie