



# VAU

## Unified Communications Security Assessment Utility

### Discovery of UC security vulnerabilities

- Network intrusion
- Denial of service
- Unauthorized wired devices
- Unauthorized wireless smartphones
- Weak or default IP-phone passwords
- Exposed interfaces
- Exposed user identities
- Exposed user directories
- Exposed numbering plans
- Weak voice/data network separation
- Weakly protected IP-phone configuration
- Weak network access control

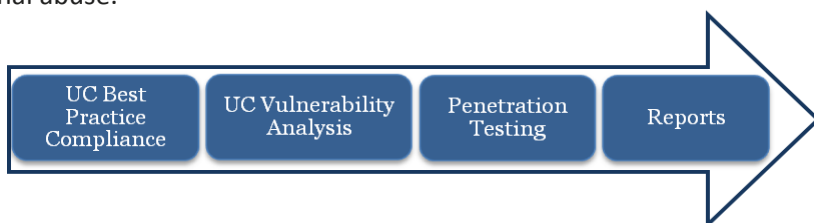
### Discovery of vulnerability to toll fraud

- Misconfigured IP-PBX calling rules
- Compromised IP-Phones
- Promiscuous branch office gateways
- Weak or default voicemail passwords
- Permissive call policies
- Unused extensions
- Permissive DISA use policies
- Weak premium destination blacklisting
- Low role-based policy granularity

### Verification of compliance

- Best practices
- Compliance with regulations
- Awareness of UC network security status
- Factual analytical and forensic reports

**VibeSec Assessment Utility™ (VAU)** is a software platform that facilitates and automates security assessment of Unified Communications and IP Telephony networks and systems. With a minimal involvement of network administration personnel the VAU will discover, analyze and report UC security issues such as network security loopholes, mis-configured IP-PBX, compromised media gateways and VoIP phones. The wizard-based, technology-assisted process enables systematic discovery and vetting of UC security, compliance and risk issues, including vulnerability of UC systems to hacking attacks, external toll fraud and internal abuse.



### Assessment methodology

The assessment is performed on the target network by the VAU operator, with a partial involvement of the administrator of the network. The VAU is typically installed on a laptop. In order to perform the assessment the operator will disconnect one of the IP-phones from a wall outlet and connect the outlet to the laptop. Depending on network architecture, several assessments may need to be performed from different points of connection to the network. The highly structured process is performed in four stages:

**Wizard-based input of information** about the existing UC/VoIP network architecture and security practices, followed by automated analysis of compliance with best practices and security standards.

**Automated discovery and assessment** of all Unified Communications assets attached to the target network, followed by analysis of their security status and vulnerability to hacking techniques.

**Automated penetration testing** (optional) to confirm and demonstrate the effects of the specific security loopholes discovered in the previous stages of the assessment process.

**Generation of audit reports** including factual, analytical and forensic reports.



The VAU self-installs from a USB memory stick on any standard Windows based computer.

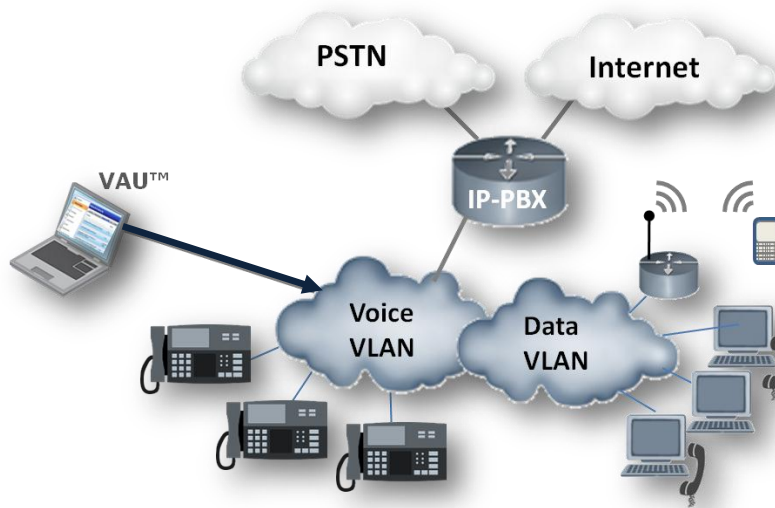
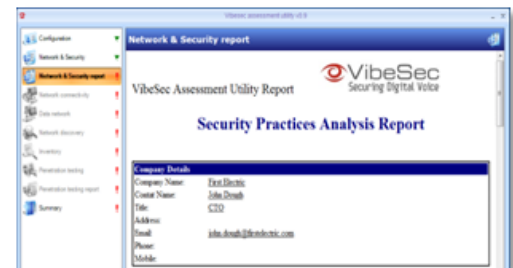
## System Requirements

- Windows XP / Vista / 7
- Local Administrator Account
- 4GByte Memory
- Network connection

[www.vibsec.com](http://www.vibsec.com)

**VibeSec Assessment Utility™ (VAU)** is based on VibeSec's breakthrough Non-Intrusive State Monitoring (NISM™) technology that enables coherent assessment of state of security and risks associated with enterprise UC systems and services in a multi-vendor environment.

Implementation of VAU - based assessment is simple and efficient, due to non-intrusive network connection and comprehensive assessment process wizard.



VibeSec Ltd.  
 MATAM-Advanced Technologies Center  
 Building #30  
 P.O. Box 15054  
 Haifa 31905, Israel  
 Tel +972-4-854-6654  
 Fax +972-4-854-6644  
 Email [info@vibsec.com](mailto:info@vibsec.com)

