

Infrastruktura VoIP z perspektywy bezpieczeństwa

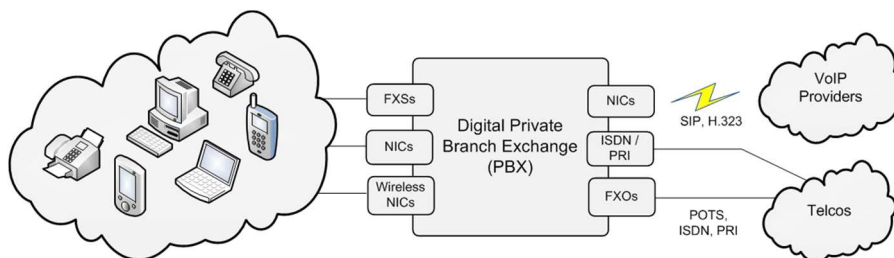
Artur Maj, Adam Nowak

Agenda

- Wprowadzenie do technologii VoIP
 - Podstawy protokołu SIP
 - Podstawy protokołu H.323
 - Podstawy protokołu RTP
 - Pozostałe protokoły
- Wybrane ataki na infrastrukturę VoIP na przykładzie protokołu SIP
- Dobre praktyki bezpieczeństwa

Wprowadzenie do technologii VoIP

Wprowadzenie do technologii VoIP



Wprowadzenie do technologii VoIP (cd.)

- Protokoły sygnalizacyjne
 - SIP (Session Initiation Protocol)
 - H.323
 - Pozostałe (przykłady)
 - IAX, SCCP (Skinny), XMPP, MGCP
- Protokoły strumieniowe
 - RTP, SRTP
- Kodeki (przykłady)
 - G.711, G.723, G.726, G.729A

Podstawy protokołu SIP

- SIP (Session Initiation Protocol)

Element	Pełniona rola
SIP User Agent	Terminal użytkownika. Może inicjować i akceptować połączenia.
SIP Registrar	Rejestracja SIP User Agent
SIP Redirect server	Przekierowuje połączenia do właściwej domeny
SIP Proxy server	Pośredniczy w zestawianiu połączeń, przesyła żądania do dalszych serwerów

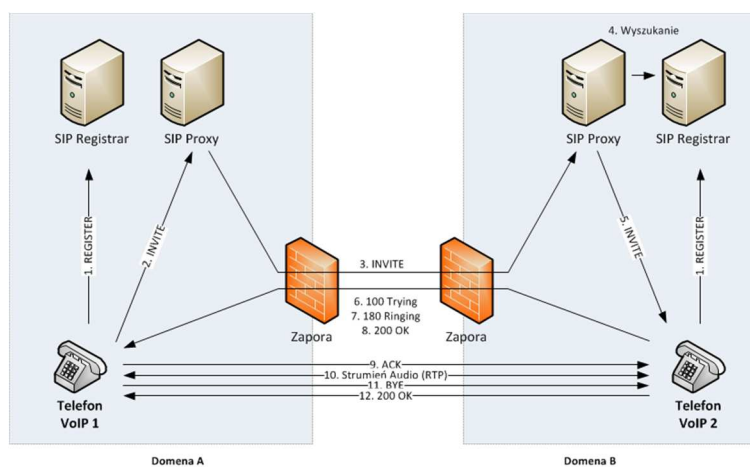
- Domyślnie nasłuchuje na portach:
 - 5060/tcp, 5060/udp

Podstawy protokołu SIP (cd.)

- Podstawowe metody protokołu SIP

Metoda	Znaczenie
INVITE	Inicjowanie połączenia
REGISTER	Rejestracja SIP User Agent w danej domenie
ACK	Potwierdzenie nawiązania połączenia
CANCEL	Anulowanie żądania połączenia
BYE	Zakończenie połączenia
OPTIONS	Określanie wspieranych metod SIP

Podstawy protokołu SIP (cd.)



Podstawy protokołu H.323

- Protokół sygnalizacyjny H.323

Element	Pełniona rola
Terminale	Terminal użytkownika. Może inicjować i akceptować połączenia.
H.323 Gatekeeper	Rejestracja i uwierzytelnianie terminali
H.323 Gateway	Trasowanie połączeń
Session Border Controller	Pomaga komunikować się przez zapory ogniowe

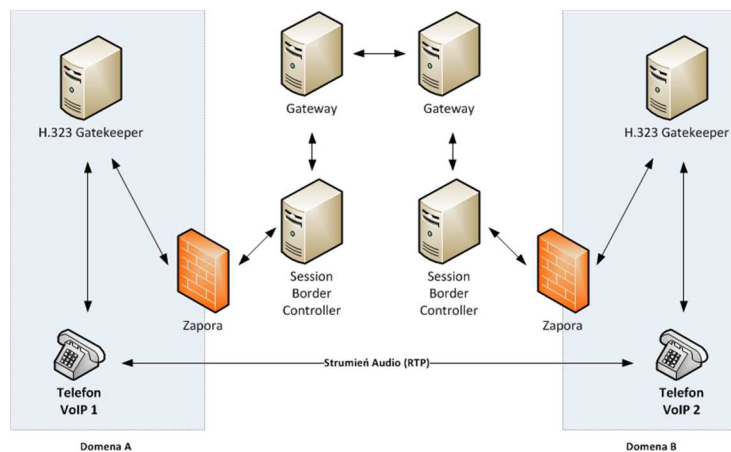
- Domyślnie nasłuchuje na portach:
 - 80/tcp, 1718-1720/tcp, 1731/tcp

Podstawy protokołu H.323 (cd.)

- Podstawowe podprotokoły H.323

Element	Pełniona rola
H.225	Zarządzanie rejestracją, dopuszczeniem, stanem
H.245	Protokół kontrolny
H.450	Usługi wspierające
H.235	Usługi bezpieczeństwa
H.239	Strumieniowanie
H.460	Obsługa zapór ogniowych

Podstawy protokołu H.323 (cd.)



© 2011 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity

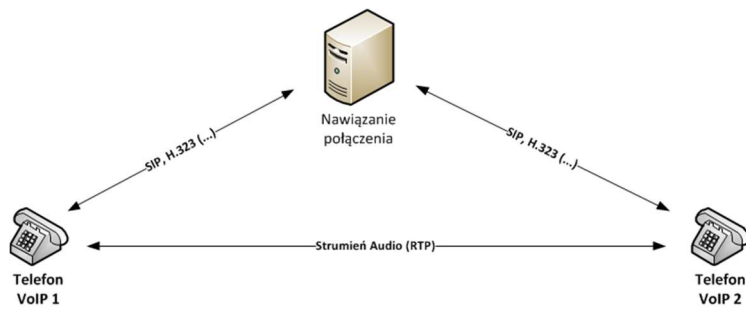
Podstawy protokołu RTP

- RTP (Real-time Transport Protocol)
- RTCP (Real-time Transport Control Protocol)
- Najpopularniejszy protokół do przesyłania multimediów dla protokołów SIP oraz H.323
- Przesyła dane w postaci otwartej
- Wykorzystuje protokół UDP, porty otwierane w sposób dynamiczny lub statyczny

© 2011 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity

Podstawy protokołu RTP (cd.)



© 2011 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity
PROFESJONALNE ROZWIĄZANIA

Wybrane ataki na infrastrukturę VoIP na przykładzie protokołu SIP

Rozpoznanie infrastruktury VoIP

- Wykrywanie serwerów i urządzeń SIP:
 - Skanowanie portów 5060-5061 TCP i UDP
 - Próby połączeń HTTP / SNMP / TELNET / TFTP itp.
 - Aktywne i pasywne rozpoznanie systemu operacyjnego
- Wykrywanie nazw użytkowników:
 - Próbki SIP Registrar i SIP Proxy
 - REGISTER
 - INVITE
 - Podśluch komunikacji SIP
 - SIP URI

Ataki na mechanizmy uwierzytelniania

- Próby rejestracji w SIP Registrar
 - Atak siłowy lub słownikowy
- Próby odgadnięcia hasła z wykorzystaniem podsłuchanego skrótu MD5
- Atak Man-In-The-Middle
 - ARP Spoofing / DNS Spoofing / DHCP Spoofing
 - Podszycie się pod SIP User Agent
- Przechwycenie rejestracji
 - Modyfikacja pola *Contact*
- Podszycie się pod serwery SIP Proxy, SIP Registrar
- Przekierowanie na podstawione H.323 Gatekeepers

Ataki na komunikację VoIP

- Podłuchiwanie i nagrywanie rozmów
 - Protokół RTP przesyła dźwięk w postaci jawnej
- „Wstrzykiwanie” lub zastępowanie dźwięku
- Dystrybucja głosowych wiadomości SPAM (tzw. SPIT)
- Uniemożliwienie działania
 - Podłuch *Call-ID* i przesyłanie komunikatów BYE
 - Wysyłanie komunikatów REGISTER i modyfikacja pola *Contact* na nieistniejący adres IP
 - Wyrejestrowanie User Agent
 - REGISTER i ustawienie czasu ważności na 0
 - Przesyłanie komunikatów RTCP BYE
 - Zalewanie urządzenia pakietami RTP

© 2011 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity

Ataki na urządzenia

- Błędy bezpieczeństwa
 - Terminale programowe i sprzętowe
 - Centralki VoIP
 - Serwery proxy
 - Inne serwery pośredniczące
 - Serwery HTTP
 - Serwery Trivial FTP

© 2011 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity

Ataki na urządzenia - przykłady

- Platforma PBX, np. Asterisk

Rok 2011:

Asterisk SIP 'REGISTER' Request User Enumeration Weakness
Asterisk Manager Interface Arbitrary Command Execution Security Bypass Vulnerability
Asterisk SIP INVITE Request User Enumeration Weakness
Asterisk TCP/TLS Server NULL Pointer Dereference Denial Of Service Vulnerability
Asterisk UPDTL Packets Buffer Overflow Vulnerabilities
Asterisk Manager Interface Remote Denial of Service Vulnerability
Asterisk SIP Channel Driver Stack Buffer Overflow Vulnerability

Rok 2010:

Asterisk RTP Comfort Noise Processing Remote Denial of Service Vulnerability
Prototype JavaScript Framework Cross-Site Ajax Request Vulnerability
Asterisk IAX2 Call Number Space Exhaustion Remote Denial of Service Vulnerability
Asterisk SIP Response Username Enumeration Remote Information Disclosure Vulnerability
Asterisk SIP Channel Driver 'scanf' Multiple Remote Denial of Service Vulnerabilities
Asterisk T.38 'FaxMaxDatagram' Remote Denial of Service Vulnerability
Asterisk CIDR Notation in Access Rule Remote Security Bypass Vulnerability
Asterisk Dialplan '\${EXTEN}' Variable String Injection Vulnerability

Źródło: www.securityfocus.com

Ataki na urządzenia - przykłady

- Telefony sprzętowe, np. Cisco CP-7960



Telefon Cisco VoIP CP-7960:

- Cisco VoIP Phone Default Administrative Password Vulnerability
- Cisco VoIP Phone Web Interface System Memory Contents Information Leakage Vulnerability
- Cisco VoIP Phone Stream Request Denial Of Service Vulnerability
- Cisco 7940/7960 Phones SIP Message Handling Remote Denial of Service Vulnerabilities
- Cisco 7940/7960 Phone SIP Invite Remote Denial of Service Vulnerability
- Multiple Vendor VoIP Phones Spoofed SIP Status Message Handling Weakness

Źródło: www.securityfocus.com

Ataki na urządzenia - przykłady

- Telefony programowe, np. X-Lite / eyeBeam



CounterPath X-Lite / eyeBeam:

- CounterPath X-Lite '.wav' File Buffer Overflow Vulnerability
- CounterPath X-Lite SIP Soft Phone Malformed Packet Denial of Service Vulnerability
- CounterPath eyeBeam SIP Header Data Remote Buffer Overflow Vulnerability

Źródło: www.securityfocus.com

© 2011 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity
SECURITY SOLUTIONS

Ataki na urządzenia (cd.)

- Wykorzystanie domyślnych lub trywialnych do odgadnięcia haseł (lub nawet ich braku)
- Wykorzystanie protokołu SNMP
- Nieautoryzowany dostęp do konfiguracji telefonów (TFTP)
- Modyfikacja lub podmiana konfiguracji telefonów
- Nieautoryzowany dostęp do skrzynki głosowej
- Zdalna kontrola nad telefonem:
 - Podsluchiwanie rozmów w otoczeniu telefonów
 - Ustawienie przekierowania rozmów

© 2011 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity
SECURITY SOLUTIONS

Demonstracja ataków

© 2011 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity
SECURITY SOLUTIONS

Dobre praktyki bezpieczeństwa

Dobre praktyki bezpieczeństwa

- Na poziomie infrastruktury i serwerów usług:
 - Separacja sieci komputerowej VoIP od sieci LAN
 - Zastosowanie i konfiguracja Quality of Service
 - Hardening serwerów wspierających usługę VoIP, m. in.:
 - Serwery DHCP / DNS
 - Serwery RADIUS / LDAP
 - Serwery TFTP / HTTP / HTTPS
 - Serwery SIP/H.323
 - Serwery Proxy
 - Obsługa protokołów VoIP na systemie firewall lub użycie Session Border Controllers (SBC)
 - Wymuszenie kontroli dostępu do sieci (np. 802.1x)
 - Centralne logowanie zdarzeń z urządzeń VoIP
 - Monitorowanie protokołu ARP

Dobre praktyki bezpieczeństwa (cd.)

- Na poziomie infrastruktury VoIP
 - Wymuszanie uwierzytelniania metod:
 - REGISTER, INVITE
 - Wymuszenie silnego uwierzytelniania
 - Wymuszenie szyfrowania połączeń
 - Protokołów sygnalizacyjnych
 - SIP: TLS lub S/MIME
 - H.323: TLS
 - Komunikacji strumieniowej
 - Secure RTP (SRTP)
 - ZRTP, IPSec
 - Wyłączanie obsługi zbędnych (lub niebezpiecznych) protokołów (np. TELNET, FTP, SNMP v1/v2) w telefonach

Dobre praktyki bezpieczeństwa (cd.)

- Ciągła aktualizacja infrastruktury o poprawki bezpieczeństwa
- Objęcie infrastruktury VoIP systemem IDS/IPS
- Wykonywanie **testów penetracyjnych**:
 - Przed zakończeniem wdrożenia VoIP
 - W okresowych odstępach czasu (np. raz na rok)

Dziękujemy za uwagę

artur.maj@prevenity.com
adam.nowak@prevenity.com