Bezpečnost v komunikacích, 2+2

Security in Communications

---

lecturer: Doc. Ing. Miroslav Vozňák, Ph.D.
seminars: Ing. Filip Řezáč

Subject Objectives
Learning outcomes are set so that the students are able to identify and apply to tasks related to the security in communications.

Anotation
This course provides an explanation of security mechanisms and solutions of voice communication in IMS systems, networks with VoIP technology and mobile networks. Students will acquire practical skills and they will be able to design and implement the particular security measures in open-source environment.

Lectures

1. Úvod do bezpečnosti, bezpečnost sítí, schéma síťového útoku, klasifikace a techniky útoků.
Introduction to security, network security, scheme for network attack, classification and techniques of attacks

2. Secure Sockets Layer, navázání SSL komunikace, OpenSSL knihovna a použití OpenSSL
Secure Sockets Layer, setting up SSL connection, Open SSL library and the using OpenSSL

3. Secure Shell, transportní a autentizační protokol SSH, SSH tunely. Autentizace v síti, systém Kerberos.
Secure Shell, SSH transport and authentication protocol, SSH tunnel. Authentication in network, System Kerberos.

4. Zabezpečení na vrstvě síťové (IPsec - AH,ESP,IKE, ISAKMP) a transportní (TLS, WTLS, DTLS)
Security on network (AH,ESP,IKE, ISAKMP) a transport layer (TLS, WTLS, DTLS)

5. Autentizace v mobilních sítích 2GPP a 3GPP (AKA – autentizační vektory, vzájemná autentizace a resynchronizace), bezpečnost bezdrátových sítí 802.11
Authentication in mobile networks 2GPP and 3GPP (AKA – authentication vectors, mutual authentication and resynchronization), security in wireless networks 802.11

6. Zabezpečení médií v IP telefonii (RTP, SRTP, DTLS-SRTP a ZRTP)
Media security in IP telephony (RTP, SRTP, DTLS-SRTP a ZRTP)

7. Autentizační mechnismy protokolu SIP a H.323
Authentication mechanisms of SIP and H.323 protocol

8. Bezpečený přístup a síťování v IMS, Session Border controler.
Secure Access and Interworking in IMS, Session Border controler

9. Uživatelská identita v SIPu, SIP SAML a P-Asserted Identity.
User Identity in SIP, SIP SAML and P-Asserted Identity

10. DoS útoky na VoIP a IMS služby
DoS attacks on VoIP and IMS Services

11. SPAM v IP telefonii, interaktivní a preventivní metody obrany
SPAM over IP telephony, interactive and preventive methods of defence

12. Zranitelnost a hrozby v komunikačních sítích
Vulnerabilities and threats in communication networks

13. Firewall, filtrování síťové a transportní vrstvy, stavová inspekce, praktické řešení s IPtables, systémy detekce a prevence průniku IDS/IPS, projekt Snort
Firewall, network and transport layers filtering, stateful inspection, practical solution with IPtables, intrusion detection and prevention systems IDS/IPS, project Snort

14. Boj proti kriminalitě na Internetu, CERT/CSIRT týmy, projekt INDECT (EU RP 7), CALEA a právní rámec v EU
Fight against criminality on Internet, CERT/CSIRT teams, project INDECT (EU FP 7), CALEA and law framework in EU

Cvičení

1. Seznámení s podmínkami absolvování předmětu, historický vývoj v oblasti zabezpečení komunikace.
2. Scannování sítě, Nmap a nalezení potencionálních bezpečnostních chyb pomocí Nessus – remote security scanner.
3. Praktické procvičení práce s OpenSSL knihovnou, vytvoření certifikační autority, generování a podepisování klíčů.
4. Implementace OpenVPN, návrh a realizace sítě.
5. Analýza šifrovacích algoritmů v OpenVPN a módu šifrování. (5 b.)
6. Implementace OpenSwan, návrh a realizace sítě.
7. Hashovací funkce – útok na MD5. Zadání referátu (případ z praxe – z oblasti bezpečnosti komunikace)
8. Zabezpečení v sítích 802.11, NetStumbler a Kismet - praktické cvičení.
9. Analýza protokolů v reálném čase – RTP, SRTP a ZRTP.
10. Analýza autentizačních mechanizmů v protokolu SIP. Zadání semestrálního projektu.
11. SPAM v IP telefonii – SIPp, SPITfile a AntiSPIT. Řešení sem. projektu.
12. Prezentace referátů zadaných na cvičení č. 7 (5 b.) a řešení sem. projektu.
13. Praktické cvičení - DoS útoky v IP telefonii a obrana na úrovni FW. (5 b.)
14. Odevzdání a předvedení semestrálních projektů (15 b.) a zápočet.

Podmínky udělení zápočtu

Student může získat max. 30 bodů, během semestru získává body za průběžné práce (max. 15 b.) a za semestrální projekt (max. 15 b.), pro udělení zápočtu musí získat min. 15 bodů.

Literatura

SISALEM,D.,FLOROIU,J. *SIP Security*. New Jersey: JWS, Inc. 350p. 2009. ISBN: 978-0-470-51636-2
COLLIER,M.,ENDLER,D. *Hacking VoIP exposed*. New York: McGraww-Hill, 539p. 2007. ISBN 978-0-07-226364-0
RANSOME,J.,RITTINGHOUSE,J*. VoIP Security*. Oxford: Elsevier, 402p. 2005. ISBN 1-55558-332-6.
LEVICKÝ,D. *Kryptografia v informačnej bezpečnosti*. Košice: Elfa, 266s. 2005. ISBN:80-8086-022-X

Doporučená literatura

PORTER,T. *Practical VoIP Security*. Rockland: Syngress Publishing, Inc., 563p. 2006. ISBN 1-59749-060-1
WALLINFORD,T. *VoIP Hacks*. OReilly Media,Inc., 306p. 2006. ISBN 0-596-10133-3.
FEILNER,M. *OpenVPN*. Birmingham: Packt Publishing,Ltd., 258p. 2006. ISBN 1-904811-85-X
PŘIBYL, J.,KODL, J. *Ochrana dat v informatice*. Praha: ČVUT v Praze, 299. 1997. ISBN 80-01-01664-1
KONHEIM,A. *Computer Security and cryptography*. New Jersey: JWS, Inc. 521p. 2007. ISBN: 978-0-471-94783-7
PŘIBYL, J. *Informační bezpečnost a utajování zpráv*.Praha: ČVUT, 2004. ISBN: 80-01-02863-1