Wireless & Mobile security Course (ENGENSEC)

Current Status Report

1 Status of Materials

Module 1. Security basics of the wireless networks.

Module 1 Lectures

#	Topic	Academic Hours	Dev.	Status of Materials
1	Wireless networks threats models.	2	AM	SG, TG, PPT, Test All contents are now being translated to English
2	Wireless networks audit tools.	2	AM	SG, TG, PPT, Test All contents are now being translated to English
3	Basic protection techniques.	2	AM	SG, TG, PPT, Test All contents are now being translated to English

Module 1 Laboratory Works

#	Topic	Academic Hours	Dev.	Status of Materials
1	RF Coverage site survey audit	4	AM	LG Content is done, translated to English. Made out in unified view now.

Module 2. IEEE 802.11* wireless networks standards security

Module 2 Lectures

#	Topic	Academic Hours	Dev.	Status of Materials
1	Security weaknesses of WEP	2	AM	SG, TG, PPT, Test All contents are now being translated to English
2	Security mechanisms in 802.11i standart	2	DK	SG, TG, PPT, Test Content is done, translated to

				English. Made out in unified view now.
3	Extended autentication protocols in WiFi	2	DK	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
4	RADIUS/TACACS+/Diameter for wireless networks. AAA services	2	DK	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
5	Many-factor authentication. Profiling services	2	DK	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
6	Wireless attacks. Wireless IPS	2	DK	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
7	Cisco TrustSec architecture	2	DK	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
8	MACsec technology. IEEE 802.1AE	2	DK	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
9	Network Level security of wireless networks. Using VPNs and Firewalls	2	AM	SG, TG, PPT, Test All contents are now being translated to English

Module 2 Laboratory Works

#	Topic	Academic Hours	Dev.	Status of Materials
1	DoS attack: Deauthentication frame flooding	2	DK	LG Content is done, translated to English. Made out in unified view now.
2	WPA/WPA2 PSK. Dictionary Attack	2	DK	LG Content is done, translated to English. Made out in unified view now.
3	WPA/WPA2 PSK. Speeding up Dictionary Attack	2	DK	LG Content is done, translated to English. Made out in unified view now.
4	WPA/WPA2 PSK. AP-Less Dictionary Attack. Honey pot	2	DK	LG Content is done,

				translated to English. Made out in unified view now.
5	Rogue AP classification	2	DK	LG Content is done, translated to English. Made out in unified view now.
6	Wireless MITM attaks using Kali Linux	4	AM	LG All contents are now being translated to English
7	Configure of firewall for wireless nework	4	AM	LG All contents are now being translated to English
8	Using VPN to secure wireless connections	4	AM	LG All contents are now being translated to English
9	Use FreeRADIUS for Wi-Fi Authentication improvement	4	AM	LG All contents are now being translated to English
10	Controller Based IDS	2	DK	LG Content is done, translated to English. Made out in unified view now.
11	Protected Management Frames (MFP/PMF)	2	DK	LG Content is done, translated to English. Made out in unified view now.
12	wIPS	2	DK	LG Content is done, translated to English. Made out in unified view now.

Module 3 Embedded and cyber-physical systems features. Bluetooth and ZigBee security.

Module 3 Lectures

#	Topic	Academic Hours	Dev.	Status of Materials
1	Embedded and cyber-physical systems features	2	BV	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view

				now.
2	Bluetooth technology and its security features	2	BV	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
3	Bluetooth vulnerability, attacks and countermeasures	2	BV	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
4	ZigBee security basics. IEEE 802.15.4 standard	2	BV	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
5	ZigBee vulnerability. Defense of ZigBee systems.	2	BV	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.

Module 3 Laboratory Works

#	Topic	Academic Hours	Dev.	Status of Materials
1	Bluetooth penetration test	4	BV	LG Content is done, translated to English. Made out in unified view now.
2	Connecting and configuring of ZigBee devices	4	BV	LG Content is done, translated to English. Made out in unified view now.
3	Attacks on ZigBee with KillerBee tools.	4	BV	LG Content is done, translated to English. Made out in unified view now.

Module 4: RFID and IR techniques security. Alarms.

Module 4 Lectures

#	Topic	Academic Hours	Dev.	Status of Materials
1	Wireless data transmission technologies in alarm systems and access control	2	BV	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
2	Radio frequency identification systems (RFID). Structure and principles of operation	2	BV	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.

3	RFID. Standards and implementation. Information security vulnerabilities	2	BV	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
4	Alarms in security systems and access control	2	BV	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.
5	Infrared (IR) sensors in security systems	2	BV	SG, TG, PPT, Test Content is done, translated to English. Made out in unified view now.

Module 4 Laboratory Works

#	Topic	Academic Hours	Dev.	Status of Materials
1	RFID reading/writing systems analysis	4	BV	LG Content is done, translated to English. Made out in unified view now.
2	IR security sensors implementation and configuration	4	BV	LG Content is done, translated to English. Made out in unified view now.
3	Wireless data transmission: imitation and detection	4	BV	LG Content is done, translated to English. Made out in unified view now.

Optional Topics:

Module 5 Mobile network security mechanisms

Module 5 Lectures

#	Topic	Academic Hours	Dev.	Status of Materials
1	GSM network security mechanisms, vulnerability, attacks and countermeasures	2	AM	SG, TG, PPT, Test All contents are now being translated to English
2	3G Mobile network security features	2	AM	SG, TG, PPT, Test All contents are now being translated to English
3	4G and beyond network security features	2	AM	SG, TG, PPT, Test Content during creation

Materials type:

SG – Students Guide
TG – Teatchers Guide
PPT – PowerPoint Presenation

Authors abbreviation:
AM – Artem Marchuk
DK – Daniil Kirillov
BV – Bogdan Voytusik

2 Overlapping of Materials

After the discussion in working groups it was established that there is no overlap of topics.

All potential overlaps in some themes were excluded due to the greater specificity of themes. For example, studying the topic of IDS in “Adv. Network & Cloud security” course does not consider WIDS, in order that would not overlap such theme in wireless course.

Other topics such as the EAP, VPN, firewalls and certain types of network attacks are considered only in the wireless case, describe its particular features and thus cannot overlap with other courses.

3. Some additions

After the discussion in the working groups we concluded that:

1. The course of “Pentest and ethical hacking (practical aspects)” should be taught before this course. This may be important for consistency of students study. Thus the students will be familiar with common methods of hacking and will get base skills in use of Kali Linux that will be desirable for this wireless course. In our course, they will implement their skills on pentest for wireless networks. Thus it will be continuation the study but applied to wireless themes.

2. It was decided that module 5 is optional. Depending on the needs of a particular university it can be taught or replaced by another theme. Also, this module can be given to students on self-study.