Úvod do informačnej bezpečnosti

Daniel Olejár

Obsah celej prednášky

- Úvod
- História
- Všeobecný základ (pojmy)
- Legislatíva a štandardy
- O úlohách štátu a ostatných zúčastnených
- Kryptológia
- Manažment informačnej bezpečnosti podľa ISO/IEC 27001
- Bezpečnosť operačných systémov a sietí
- Ochrana pred škodlivým softvérom
- Elektronický podpis a PKI
- Audit
- Bezpečnostný projekt

Úvod (1)

- Neštandardná prenáška
- Doteraz – matematika, informatika, konkrétne IKT, možno aj spoločenské aspekty informatiky (prednášky s dobre definovaným predmetom)
- Informačná bezpečnosť je (ako uvidíme) iná
- Cieľ informačnej bezpečnosti – aby IKT systémy dobre fungovali
- Nutnosť riešiť technické, informatické, organizačné, právne, ekonomické, psychologické a iné problémy
- Zatiaľ nie je samostatný vedný odbor, ale je to multidisciplinárna oblasť
- Napriek tomu vo svete existujú špecialisti na informačnú bezpečnosť a niekoľko systémov ich prípravy

Úvod (2)

- InfoSec na FMFI – od začiatku 90. rokov (rozličné predmety, diplomovky, dizertácie)
- Posun - InfoSec ako súčasť povinného základu informatického vzdelania
- Realizácia - táto prednáška
- Cieľ: prehľad
  - Čo je informačná bezpečnosť
  - Aké problémy rieši
  - Akými metódami
  - Kde sa dozviem viac
- Absolvent prednášky: bezpečnostne poučený informatik, nie špecialista na informačnú bezpečnosť

Úvod (3)

- Obsah prednášky
  - Všeobecný základ a tématické bloky
  - Tématické bloky budú prednášať špecialisti
- Prednáška = úvod do problematiky a odporúčané informačné zdroje pre samostatné štúdium (literárne alebo internetové zdroje)
- Cvičenia ani kontrola počas semestra nie sú
- Skúška
  - Malá verzia CISA/CISM skúšky
  - Technické otázky – O.K., iné – problém
  - Treba aj rozmýšľať
  - Najlepší výsledok – špeciálny bonus – stáž v profesionálnej firme
- Upozornenie
  - Angličtina je nevyhnutnosťou
  - Prezentácie z prednášky na skúšku nepostačujú
  - Na získanie a udržanie poznatkov treba samostatne a systematicky študovať

Čo vlastne je informačná bezpečnosť?

Prednáška č. 1

Obsah

- Význam informačnej bezpečnosti
- Vymedzenie obsahu InfoSec
- Čo sa od nás očakáva?
- História informačnej bezpečnosti
- Základné pojmy

Čo je informačná bezpečnosť a prečo ju potrebujeme?

- Úloha informácie a informačných technológií v ľudskej spoločnosti
  - Kolektívne poznanie, kumulácia poznania
  - Koordinácia činnosti
- Reč, písmo, tlač, komunikačné systémy, rozhlas, televízia, počítače, médiá
- Automatizované spracovanie informácií - zavádzanie IKT a informatizácia spoločnosti
- Závislosť spoločnosti od IKT
- Dôsledky zlyhania, výpadku, poškodenia IKT
- IKT budú plniť svoje poslanie len ak budú fungovať
- Informačná bezpečnosť :
  - Stav IKT systémov
  - Interdiscipliárna oblasť zaoberajúca sa ochranou IKT a informácie, ktorá sa v nich spracováva
- Týka sa všetkých zúčastnených
- Nedá sa riešiť jednorazovo
- Vyžaduje netriviálne know-how

Prečo ja?

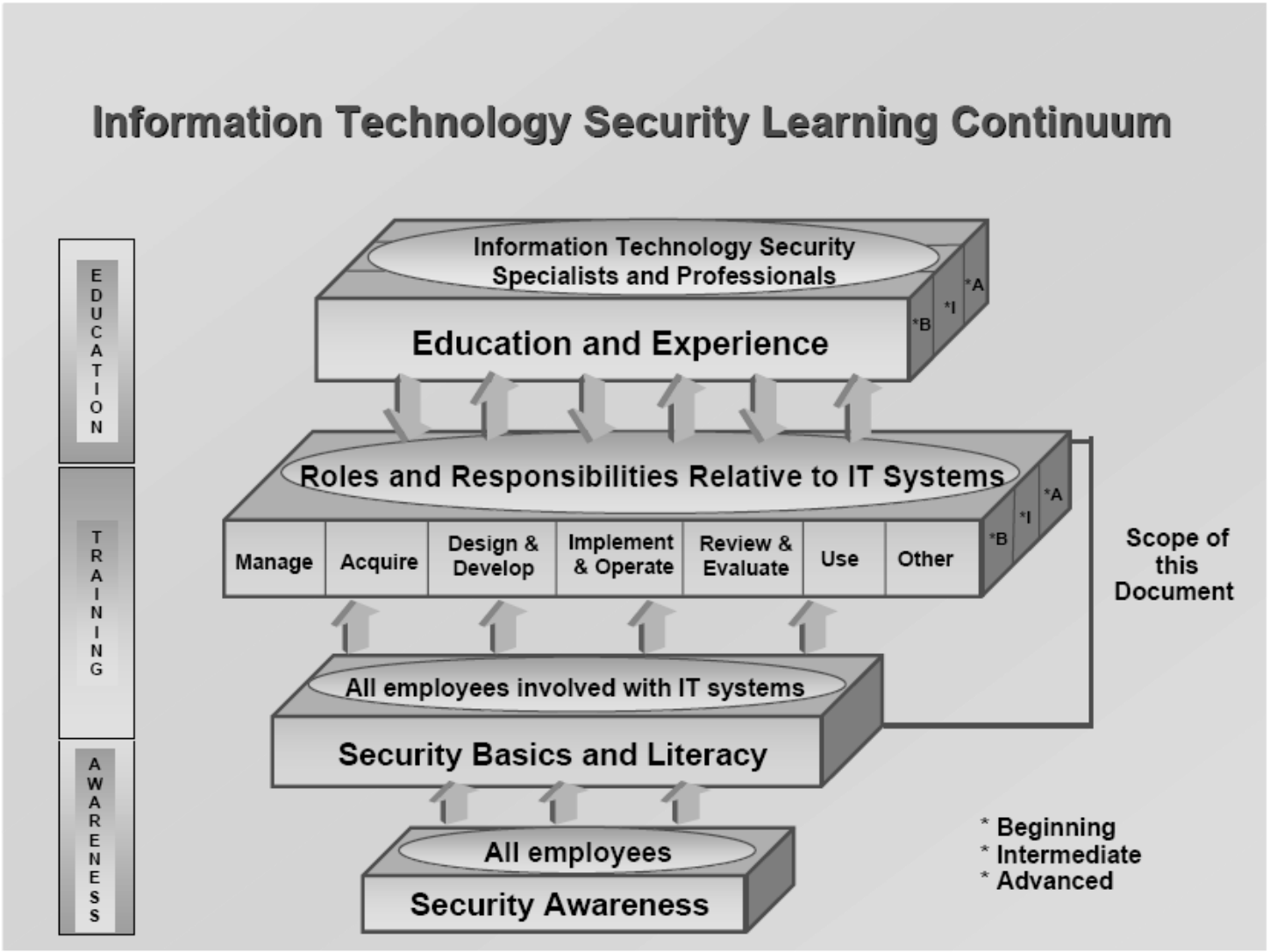
- The (US) National Strategy to Secure Cyberspace

  Everyone who relies on part of cyberspace is encouraged to help secure the part of cyberspace that they can influence or control. To do that, users need to know the simple things that they can do to help to prevent intrusions, cyber attacks, or other security breaches. All users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace.

Kde asi sme v digitálnom priestore a čo sa od nás očakáva?

- Štúdia Návrh systému vzdelávania v informačnej bezpečnosti v SR (2009):
  - laici – osoby, ktoré sú primárne používateľmi IKT
  - manažéri a vedúci pracovníci – osoby vo vedúcom postavení, ktoré okrem používania IKT zodpovedajú za riadenie inštitúcií prevádzkujúcich IKT
  - informatici nešpecialisti v informačnej bezpečnosti – osoby, ktoré sa aktívne podieľajú na návrhu, vývoji alebo prevádzke IKT, pričom bezpečnosť nie je hlavnou náplňou ich práce
  - špecialisti v informačnej bezpečnosti – osoby, ktoré sa profesne zaoberajú bezpečnosťou IKT, či už jej posudzovaním, riadením, riešením incidentov a pod.
  - výskumníci v informačnej bezpečnosti – osoby rozvíjajúce poznanie v oblasti informačnej bezpečnosti
  - učitelia – osoby poskytujúce vzdelávanie v oblasti informačnej bezpečnosti

Exhibit 2-1
IT Security Learning Continuum



Čo by sme mali vedieť?

- pochopenie hrozieb, zraniteľností a výsledných rizík spojených s IKT systémami, mechanizmov a opatrení na ich elimináciu alebo redukciu, ako aj predpokladov a dôsledkov ich realizácie
- pochopenie podstaty bezpečnostných požiadaviek na IKT systém a možností ich naplnenia
- schopnosť navrhnúť, realizovať, udržiavať a prevádzkovať (v súlade s príslušnou profesnou orientáciou) mechanizmy na naplnenie bezpečnostných požiadaviek na IKT systém
- schopnosť byť kvalifikovaným partnerom pre spoluprácu so špecialistami v informačnej bezpečnosti (tam, kde sa profesné orientácie prekrývajú)

História informačnej bezpečnosti (1)

- Samostatná kapitola informačnej bezpečnosti je kryptológia a komunikačná bezpečnosť
- Kahn D. The Codebreakers, Scribner, New York 1996
- 2. svetová vojna (Enigma, Purple)
- Rozvoj telekomunikácií (nelegálne telefonovanie)
- Počítače a elektronické IKT
  - (obdobie 1950-1975) počítačové sály
  - Terminály, lokálne siete, fyzická ochrana nepostačuje
  - 80-te roky – prepojenie cez modemy a telefónne linky
  - Nové služby bulletin board service (BBS)
  - Koniec 80-tych rokov PC a Internet

História informačnej bezpečnosti (2)

- Prvý červ (Morris 1988) http://en.wikipedia.org/wiki/Morris_worm
- CERT http://www.cert.org/
- Hackeri
- Vírusy a iná háveď
- Nedávna minulosť a súčasnosť
  - Elektronický obchod
  - Profesionalizácia útočníkov
  - Ekonomické motívy
  - Kriminálne živly a teroristi
  - špionáž

História informačnej bezpečnosti (3)

Aktuálne problémy (BSI)

- Poruchy systémov a infraštruktúry
- Bezpečnostné diery
- Zlomyseľný softvér
- DoS útoky
- Nevyžiadaná pošta
- Bot-nets
- Phishing a krádeže identity
- Vlastní zamestnanci, chyby a nedbalosť
- Outsourcing

História informačnej bezpečnosti (4)

- Politický dosah
  - USA (podrobnejšie pri legislatíve a štandardoch)
  - EÚ – informatizácia spoločnosti (e-Europe, i-Initiative)
- Echelon a UKUSA
- Kritická infraštruktúra spoločnosti
- Komplexný a koordinovaný prístup k ochrane IKT
- Budúcnosť ???

The Big Brother

- November 1999, WASHINGTON (NWS) -- The U.S. Navy is supporting new speech recognition research for its potential benefits to Navy sonar. Biomedical engineers at the University of Southern California have created the world's first machine system that can recognize spoken words better than humanscan. In benchmark testing, USC's speech recognition system bested all existing computer systems and outperformed the keenest human ears. The system may eventually advance voice control of computers and other machines, help the deaf, aid air traffic controllers and others who must understand speech in noisy environments, and instantly produce clean transcripts of conversations, with each speaker correctly identified.

a ekonomika ...

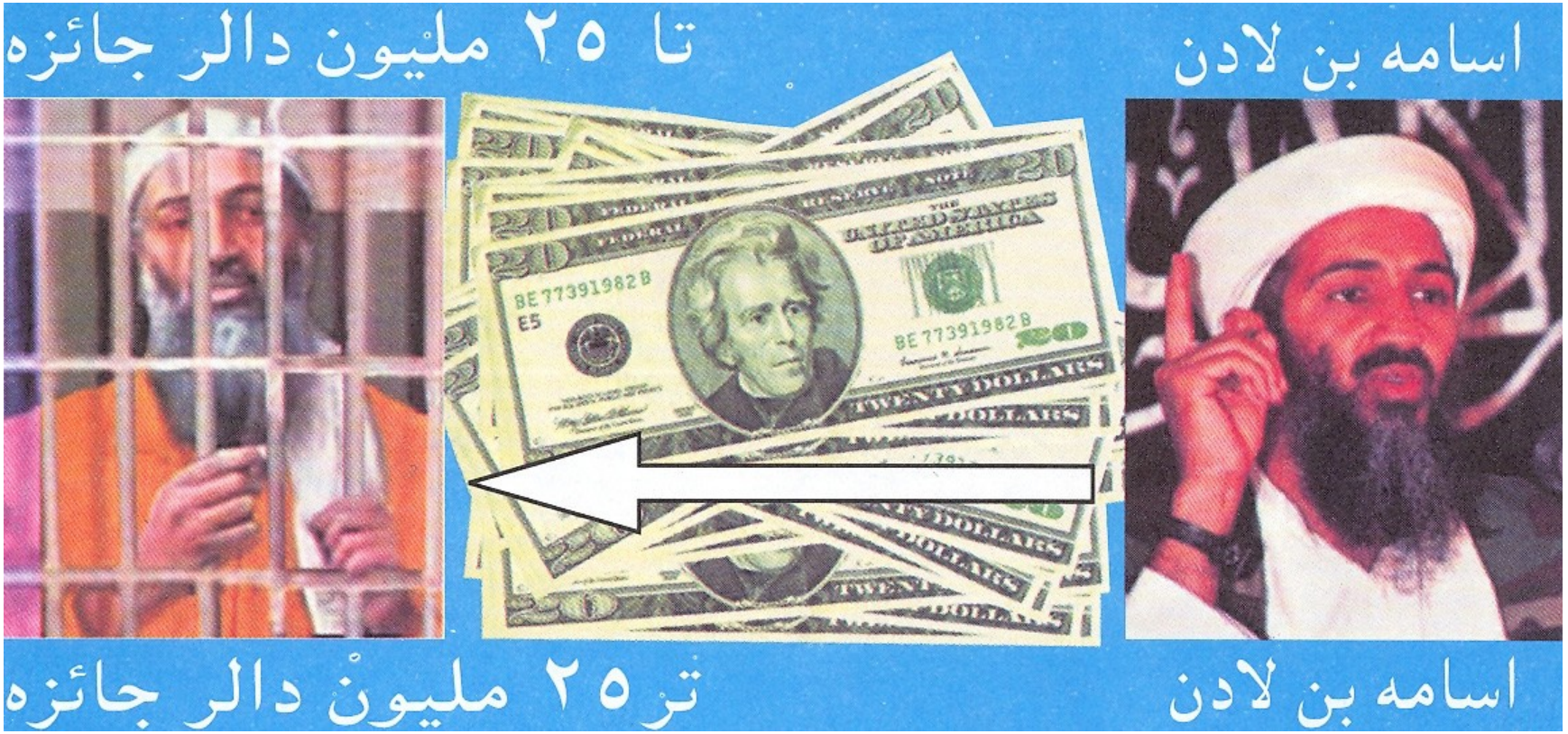
- some examples of the misuse of economic information intercepted by global networks such as *ECHELON.*
  - We can actually quote the contract which was spirited away from France in January 1994. It involved an arms supply contract worth 30 million francs with Saudi Arabia. The contract ended up with McDonnell-Douglas, the rival of the Airbus consortium, because the former was privy to the financial terms offered by Airbus thanks to the electronic interception system.
  - that ECHELON has been used to benefit American companies involved in arms contracts and to strengthen Washington´s hand in major negotiations with Europe in the World Trade Organisation in relation to disputes with Japan concerning the export of motor vehicle spare parts.
  - the French electronics giant, Thomson, had lost a contract worth 1.4 million dollars for the supply of a surveillance system to Brazil because the Americans had intercepted details of the negotiations and passed them on to the US Raytheon Corporation, which subsequently won the contract.

Terorizmus (1)

- Cyberterrorism is defined as “The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives.” (Kevin G. Coleman of the Technolytics Institute.)

Terorizmus al Qaeda(2)

...and the other side



Terorizmus (3)

- Potenciál veľký, hrozba zatiaľ reálne nenaplnená (výnimka Estónsko, možno NIMDA)
- Aktraktívny
  - Anonymita
  - Potenciál spôsobiť veľké škody
  - Psychologický dopad
  - Príťažlivá téma pre médiá
- Cyberterrorism spája dve obavy
  - Možnosť stať sa náhodnou obeťou
  - Strach z počítačových technológií
- Médiá preháňajú (Dan Brown Digital Fortress)
- Kritické informačné systémy sú chránené (aj air gap)

Estónsko

- V apríli 2007 chceli v Talline premiestniť sochu a hrob neznámeho vojaka
- Protesty ruskej minority
- Denial od service attack na vládne systémy, banky, noviny, telekomunikačných operátorov
- Na webe premiéra Andrusa Ansipa – zverejnený falošný ospravedlňujúci list
- Predpoklad – Rusi, sa nedokázal
- Pôvodca nebol odhalený, v januári obvinili jedného človeka (Dmitri Galushkevich) za účasť na útoku, dostal pokutu asi 1600 USD
- http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
- Estonia has urged its allies in the European Union and NATO to take firm action against a new mode of warfare

Základné pojmy

- Skôr, ako budeme pokračovať, pripomenieme aspoň stručne základné pojmy informačnej bezpečnosti
  - IKT systém, jeho aktíva, bezpečnostné okolie, hrozba, zraniteľnosť, riziko, nositeľ hrozby, útok
  - Údaje a informácia
  - Bezpečnostné aspekty informácie (dôvernosť, integrita, dostupnosť, autentickosť a i.)
  - Analýza rizík, ohodnotenie rizík, návrh a implementácia opatrení, zvyškové riziko, správa rizík
  - Kontinuita činnosti, zotavenie po katastrofách
  - Bezpečnostná politika, systém riadenia informačnej bezpečnosti
- K týmto pojmom sa ešte vrátime