Univerza v Mariboru

FERI Fakulteta za elektrotehniko, računalništvo in informatiko

Inštitut za informatiko

OTS 2010
Sodobne tehnologije in storitve

in

OWASP
The Open Web Application Security Project

http://www.owasp.org

Zbornik petnajste konference

Uredniki
Marjan Heričko, Aleš Živkovič in Katja Kous

Maribor, 15. in 16. junij 2010

Pokrovitelji:

Medijski pokrovitelji:

V sodelovanju z:

OTS 2010

SODOBNE TEHNOLOGIJE IN STORITVE

in

http://www.owasp.org
http://www.owasp.org/index.php/Slovenia

VSEBINA

Sreda, 16.6.2010, OB 16:15

PASTI PRI VGRADNJI KRIPTOGRAFIJE V APLIKACIJSKI SVET

Marko Hölbl

Fakulteta za elektrotehniko, računalništvo in informatiko
Smetanova ulica 17, 2000 Maribor
e-pošta: marko.holbl@uni-mb.si

Povzetek

Kriptografija je temeljen vidik informacijske varnosti. Večinoma se ne zavedamo, da kriptografijo uporabljamo pri vsakodnevnem delu. Pogosto zasledimo novice o napadih na kriptografijo in večinoma vzrok ni v slabosti algoritmov, ampak v napakah pri implementaciji ali uporabi. V članku bomo predstavili tveganja pri vpeljavi kriptografije v aplikacije. Prikazati želimo, da je potrebno biti pri vpeljavi zelo pazljiv, saj lahko le na tak način zagotovimo, da bo kriptografija res služila svojemu namenu.

1. UVOD

Kriptografija je tehnologija, ki omogoča prikrivanje podatkov, prenesenih po nevarnih kanalih kot je internet ali brezžično omrežje. Zagotavlja zaupnost, torej berljivost le tistim, ki so pooblaščeni za dostop. To dosežemo s šifriranjem podatkov. Vendar kriptografija, kljub prepričanju, da zajema samo šifriranje podatkov, omogoča tudi overjanja in zagotavljanje celovitosti podatkov. Kriptografija ne vključujejo samo šifriranja podatkov, temveč tudi ostale gradnike, kot so zgoščevalne funkcije, algoritme za digitalno podpisovanje in varnostne protokole. V teoriji so algoritmi varni, a se pogosto zalomi pri vpeljavi v aplikacije. Na internetu pogosto zasledimo novice o napadih na kriptografijo, bodisi na šifre bodisi na druge gradnike. V večini primerov problem ne tiči v slabostih algoritmov, ampak v napakah pri implementaciji in/ali vpeljavi le-teh. Posledica je delno ali popolno razkritje podatkov, pridobitev kriptografskega ključa ali bližnjice, ki omogočajo, da napadalec zaobide varnostne mehanizme. V slednjem primeru nam tudi nezlomljiv kriptografski algoritem ne koristi.

V članku bomo predstavili pasti pri vpeljavi kriptografije v prakso tako z vidika razvijalca kot končnega uporabnika. Pogosta tematika različnih spletnih strani in blogov na temo varnosti so ravno incidenti in razkritja, ki se dogodijo v povezavi s kriptografijo, tako s končnimi izdelki (aplikacijami), kakor tudi s slabo zasnovanimi gradniki in knjižnicami. Napaka v implementaciji gradnika ali knjižnice lahko povzroči ranljivost rešitve, ki uporablja ta gradnik ali knjižnico.

Po kratkem uvodu v pojem kriptografije v poglavju 2, bomo v 3. poglavju predstavili pasti. Sledi opis smernic pri implementaciji kriptografije, ki so povzete in združene po priporočilih projekta OWASP in Ameriške vladne organizacije NIST. Članek zaokrožimo v zaključku.

2. KRIPTOGRAFIJA

Med naloge kriptografije sodijo poleg zagotavljanja zaupnosti, tudi zagotavljanje overjanja, ne-zanikanje in celovitost. Zaupnost pomeni, da so podatki dostopni samo tistemu, kateremu so namenjeni in je pooblaščen za dostop. Samo oseba ali sistem, ki je v lasti ustreznega ključa, lahko dostopa do podatkov. Zagotavljanje zasebnosti je bila prvotna naloga kriptografije, ki je omogočala preprečevanje prisluškovanja, varovanje tajnih informacij ali šifriranje gesel. Vendar se je skozi čas spekter nalog kriptografije razširil. S pomočjo sodobne kriptografije lahko preverjamo pristnost uporabnikov ali sistemov, ki so vključeni v komunikacijo. Na široko se uporablja v sodobnih varnostnih protokolih kot je SSL/TLS [11]. Zaradi možnosti zagotavljanja ne-zanikanja s pomočjo digitalnega podpisa, lahko kriptografijo uporabljamo tudi v e-poslovanju. Ne-zanikanje je koncept, pri katerem podpisnik, ki je podatke digitalno podpisal, teh kasneje ne more zanikati. Podpis pogodbe z digitalnih podpisom je po slovenski zakonodaji celo enakovreden lastnoročnemu podpisu [19]. V času interneta in brezžičnih povezav pa kriptografija deloma opravlja tudi nalogo zagotavljanja celovitosti. Tako želimo preprečiti, da nekdo spremeni podatke, ali zagotoviti, da bo vsaka sprememba podatkov opažena. Omenjeno nalogo opravljajo zgoščevalne funkcije, ene izmed temeljnih gradnikov kriptografije.

2.1. Gradniki kriptografije

Med najbolj pogosto uporabljene gradnike kriptografije zagotovo sodijo šifrirni algoritmi (ang. Encryption Algorithms) ali šifre (ang. Ciphers). Ti s pomočjo skrivnega ključa ali para ključev zagotavljajo zaupnost podatkov. Simetrični šifrirni algoritmi (ang. Symmetric Ciphers), med katere sodijo bločne šifre (angl. Block Ciphers) in tokovne šifre (ang. Stream Ciphers), uporabljajo en, skriven ključ za šifriranje in dešifriranje podatkov. Med bolj znane bločne šifre sodita DES [7] in AES [8], med tokovne RC4 [9]. Glavna težava simetričnih šifer je distribucija ključev, saj moramo ključ dostaviti od nekoga, ki je podatke šifriral do nekoga, ki jih želi dešifrirati. Problem rešujejo asimetrične šifre (ang. Asymmetric Ciphers), imenovane tudi kriptografija javnega ključa (ang. Public Key Cryptography). Ti algoritmi uporabljajo par ključev; javni ključ (ang. Public Key) za šifriranje podatkov in zasebni ključ (ang. Private Key) za dešifriranje podatkov. Ključa sta med seboj povezana tako, da je mogoče le z ustreznim zasebnim ključem dešifrirati podatke, ki smo jih šifrirali z njegovim javnim ekvivalentom. Prav tako ni mogoče s pomočjo javnega ključa pridobiti zasebnega in obratno. Glavna pomanjkljivost teh algoritmov je njihova zapletena matematična zasnova in posledično počasnost v primerjavi s simetričnimi algoritmi.

Med zelo pogosto uporabljene gradnike kriptografije sodijo zgoščevalne funkcije (ang. Hashes) in digitalni podpisi (ang. Digital Signatures). Prvi se uporabljajo za kreiranje prstnih odtisov podatkov, kar pomeni, da ima vsak poljuben niz podatkov lastno zgoščevalno vrednost in tudi če spremenimo samo delček niza, zgoščevalna vrednost ni več veljavna. Dodatno lastnost zgoščevalnih algoritmov je ta, da je praktično nemogoče najti dva poljubna niza podatkov, ki bi imela enako zgoščevalno vrednost oz. je verjetnost tega zelo majhna. Če bi želeli najti dva poljubna niza podatkov z isto zgoščevalno vrednostjo dolžine 160 bitov, bi potrebovali približno $2^{-80} = 8*10^{-25}$ poskusov. V e-poslovanja se uporabljajo algoritmi za digitalno podpisovanje. Po slovenski zakonodaji so enakovredni lastnoročnim podpisom in zagotavljajo celovitost, ne-zanikanje in overjanje podpisnika. Algoritmi kot sami se praktično ne uporabljajo, ampak se uporabljajo v kombinaciji z overjenimi digitalnimi potrdili (ang. Certificates). Algoritmi za digitalno podpisovanje so dejansko prilagojeni asimetrični šifrirni algoritmi, pri katerih je vloga ključev obrnjena. Za kreiranje digitalnega podpisa uporabimo

zasebni ključ podpisnika, za preverjanje pa njen/njegov javni ključ. V praksi ne podpisujemo celotenega niza podatkov, ampak izvleček, ki ga dobimo s pomočjo zgoščevalne funkcije.

3. PASTI KRIPTOGRAFIJE

Kriptografijo je, vsaj v teoriji, težko razbiti. Vendar pogosto zasledimo poročila o razbitju šifre ali drugega kriptografskega algoritma. V teh smernicah pa ni zapisano, da pogosto niso za razbitje krivi algoritmi oz. kriptografija, ampak napačna uporaba ter napake pri implementaciji in sami vpeljavi. V razdelku bomo predstavili najbolj pogoste ranljivosti in napake, ki se dogajajo pri implementaciji in uporabi kriptografije.

3.1. Napačna raba algoritmov

Najbolj osnoven problem, ki ga srečamo pri uporabi kriptografije, je napačna uporaba algoritmov oz. raba ranljivih ali zastarelih algoritmov. Tekom časa se pri določenih algoritmih pojavi ranljivost. Zaradi napredka v strojni opremi se dolžine ključev, ki zagotavljajo dovolj dober nivo varnosti, povečajo. DES je simetrični šifrirni algoritem, ki za današnje razmere ni več uporaben, saj je dolžina njegovega ključa prekratka (56 bitov), kar omogoča napad s poskušanje vseh možnih kombinacij; t.j. napad z grobo silo (ang. Brute Force Attack). Tudi številni zgoščevalni algoritmi se odsvetujejo zaradi pomanjkljivosti (zgoščevalni algoritem MD5 [9] ali SHA-0 [9]) ali pa zaradi napredka na področju analize teh algoritmov (algoritem SHA-1 [9]). Varnost algoritmov merimo z dolžino ključa oz. pri zgoščevalnih algoritmih dolžina izvlečka. Varen simetrični algoritem mora imeti dolžina ključa vsaj 128 bitov (dolžina ključa za doseganje visokega nivoja varnosti vsaj 192 bitov), asimetrični algoritem vsaj 1280 bitov (visok nivo varnosti vsaj 2048 bitov). Zgoščevalne funkcije naj bi imeli dolžino izvlečka (ang. Hash) vsaj 128 bitov (visok nivo varnosti vsaj 256 bitov). Omenjene številke je potrebno upoštevati pri vpeljavi. Prav tako je včasih smotrno vzeti večje dolžine ključev in malce počasnejše algoritme in s tem povečati nivo varnosti. Vendar pa s tem upočasnimo delovanje.

3.2. Nepravilnosti povezane s ključi (in digitalnimi potrdili)

Pogosta varnostna vrzel pri uporabi kriptografije je nepravilno shranjevanje in zaščita ključev in digitalnih potrdil. V praksi se ključi uporabljajo za šifriranje podatkov, medtem ko se pri digitalnem podpisovanju uporabljajo digitalno potrdila, ki vsebujejo ključ in podatke o imetniku. Če se napadalec dokoplje do ključa ali digitalnega potrdila, ne pomaga še tako napreden algoritem. Zato je potrebno ključe in digitalna potrdila varovati z močnim geslom ali jih hraniti na zunanjem varnem nosilcu kot je pametna kartica. Tudi datoteke, v katere izvozimo dig. potrdila ali ključe, je potrebno varovati z ustreznim geslom. Neustrezno je, če so ključi zakodirani v programski kodi. Ko je potreben višji nivo varnosti ključe ali digitalna potrdila hranimo na zunanjem zaščitenem nosilcu.
Pogosta tarča napada so komunikacijski kanali, ki so nezaščiteni in včasih uporabljeni za prenos zaupnih informacij, med drugim tudi ključev ali dig. potrdil. Za prenos takšnih informacij je nujno, da zaščitimo komunikacijski kanal s pomočjo ustreznega protokola (SSH [10], SSL/TLS [11], ipd.).
V povezavi s ključi svojo vlogo opravljajo tudi uporabniki. Ti se morajo zavedati svoje odgovornosti pri varovanju in upravljanju s ključi in digitalnimi potrdili, saj je razkritje najbolj preprost način, da zaobidemo kriptografske algoritme. Za pridobitev digitalnega potrdila ali ključa se napadalci vedno bolj pogosto poslužujemo tehnik socialnega inženirstva.

3.3. Nevarnost povezane z implementacijo algoritmov

Kljub temu da so kriptografski algoritmi »v teoriji« varni, se pogosto zgodi, da pa implementacije ne dosegajo enakega nivoja varnosti. Ko uporabljamo končne programske izdelke, gradnike ali knjižnice je pomembno, da posegamo po že uveljavljenih. S tem precej zmanjšamo možnost napak in nepravilnosti v implementaciji. Vendar tudi uveljavljene implementacije niso imune na napake. Primer je incident z OpenSSL knjižnico [3], ki le potrjuje kako velike razsežnosti lahko ima takšen incident. Tudi operacijski sistemi prispevajo svoje, kot se je izkazalo 2 leti nazaj pri navezi TrueCrypt [12] in Windows Vista [4, 6]. V preteklih različicah priljubljenega kriptografskega programa za končne uporabnike TrueCrypt [12] je prišlo do napak, ki so povzročile ranljivost [5].

Varnostnih vidik integracije kriptografije v aplikacije zajema tudi metodo, ki jo bomo poimenovali bližnjica. S pomočjo te metode lahko zaobidemo še tako dobro implementiran algoritem, saj izkoriščamo uhajanje podatkov (preko t.i. stranskih kanalov) ali uporabo podatkov, ki smo jih pridobili z drugo metodo (npr. kraja seje) [20]. Bližnjica omogoča neposreden dostop do varovanih podatkov ali povezav. Pogosta tarča takšnega napada je na primer pridobivanje ključa, kar omogoča dešifriranje podatkov. Zato velja pravilo, da je potrebno shranjevati najmanjšo možno mero podatkov, ki jih potrebujemo.

Uveljavljene knjižnice in gradnike je zmeraj potrebno v svoji rešitvi temeljito testirati. V primeru, da se za določen gradnik ali knjižnico pojavijo luknje, je potrebno ustrezno ukrepati in namestiti popravke ali uporabiti alternative. Tudi pri uveljavljenih knjižnicah se pojavijo pomanjkljivosti, a v primeru dovolj hitrega ukrepanja, te ne predstavljajo prevelikega tveganja.

3.4. Pasti povezane z neozaveščenostjo in pomanjkljivim znanjem

Ker so kriptografski algoritmi precej zapleteni, prihaja do težav in posledično napak pri implementaciji in uporabi. Pomembno je, da razvijalci razumejo delovanje in koncepte, ki se skrivajo za kriptografijo, tudi če knjižnice ali gradnike samo uporabljajo. Z napačno uporabo kriptografije (kot primer navedimo uporabo napačnega načina šifriranja), lahko odpro luknje. Pogosto uporabniki napačno razumejo koncepte kriptografije in zaradi tega, na primer, nepravilno ravnajo in varujejo ključe. Med razvijalci je priporočljivo vpeljati standardne procedure, ki zmanjšujejo možnosti napak pri uporabi in implementaciji kriptografije [13].
Zavedati se je treba, da napadalci izkoriščajo najšibkejši člen obrambe, ki je seveda človek. Ravno iz tega razloga je potrebno uporabnike ustrezno »pripraviti«, da ne nasedajo napadalcem. Kot že omenjeno, napadalci uporabljajo tehnike socialnega inženirstva, saj je tako najlažje razbiti kriptografijo in na tak način preprosto pridobijo ustrezen ključ.

3.5. Težava naključnih števil

Še zadnji pomemben dejavnik tveganja je generator psevdonaključnih števil. Večina kriptografskih algoritmov temelji na predpostavki, da lahko generiramo dobra psevdonaključna števila. Zato je pomembno, da pri implementaciji algoritmov oz. rešitev preverimo ali so implementacije preizkušene in varne. V preteklosti so se namreč že pojavile ranljivosti v implementaciji lastnih rešitev, ki so bile posledica slabo implementiranega generatorja psevdonaključnih števil [16, 17, 18].

4. SMERNICE ZA VARNO IMPLEMENTACIJO KRIPTOGRAFIJE

Pri implementaciji kriptografije v programske rešitve je mogoče uporabiti smernice, ki jih izdajata projekt OWASP [1, 2] in ameriška vladna agencija NIST [13]. Deloma smo smernice že obravnavali v prejšnjem poglavju. Kljub temu bomo na kratko povzeli ključne :

1. Pazite, če se pojavijo morebitne napake in varnostne pomanjkljivosti med prehodom iz faze testiranja v fazo produkcije.
2. Uporabljajte uveljavljene implementacije, saj je možnost napak manjša, pri čemer uporabite algoritme, ki se smatrajo kot močni.
3. Hranite samo podatke, ki jih resnično potrebujete.
4. Bodite pazljivi pri uporabi generatorjev psevdonaključnih števil.
5. Uporabite močne načine šifrirnih algoritmov [14] (načini OFB, CFB ali CBC).
6. Ponudite dobro dokumentacijo in izobraževanje vsem, uporabnikom in razvijalcem. Poudarek naj bo na pravilni implementaciji (za razvijalce) in pravilnemu upravljanju s ključi (za oboje).
7. Kriptografski ključi naj bodo pravilno in zadostno varovani.
8. Varnostno kritične kriptografske ključe, digitalno potrdila in druge občutljive informacije hranite na varnih zunanjih nosilcih, kot je pametna kartica in jih ustrezno zaščitite (na primer s PIN kodo).
9. Ključi in digitalna potrdila morajo imeti omejen čas veljavnosti, ki je odvisen od njihove pomembnosti (bolj pomembna digitalna potrdila in ključi morajo imeti krajši rok veljave).
10. Varujte centralna ali jedrna digitalna potrdila in ključe, ki se uporabljajo za izdajanje digitalnih potrdil in ključev uporabnikom. Dosledno beležite uporabo teh ključev.
11. Digitalna potrdila in ključe, ki niso več veljavni, je potrebno arhivirati, da lahko kasneje preverjajte podpis ali dešifrirate podatke, ko ključi več niso v uporabi.
12. Uporabniki se morajo zavedati odgovornosti v povezavi s ključi in pomembnosti varovanja ključev.
13. Šifrirajte in/ali digitalno podpišite vse pomembne podatke kot so ključi, saj s tem zagotavljate zaupnost in celovitost.
14. Za varovanje delov programske kode, ki so zadolženi za kriptografijo, lahko uporabite digitalni podpis.
15. Gesla shranjujete v obliki izvlečkov s soljo [15] (ang. Salted Hashed Passwords).

Navedene smernice ne pokrivajo vseh vidikov in tveganj, ki jih je potrebno upoštevati pri vključevanju kriptografije v rešitve, a zajemajo precejšnji del najbolj pogostih napak, ki se pojavljajo pri implementaciji kriptografije.

5. ZAKLJUČEK

V članku smo predstaviti pasti in dobre prakse pri implementaciji kriptografije v prakso. Najbolj pogoste pasti pri vgradnji kriptografije na področjih rabe algoritmov vključujejo napake povezane s ključi, nezadostno izobraževanja in napake pri implementaciji. Prav tako smo predstavili smernice povzete po projektu OWASP ter agenciji NIST, ki na kratko podajajo ključne probleme, na katere moramo biti pazljivi pri vpeljavi kriptografije v aplikacije. Tudi pri uporabi uveljavljenih izdelkov, rešitev, gradnikov ali knjižnic je potrebno biti pazljiv, saj lahko napaka pomeni ranljivost v naboru aplikacij. Če se pojavijo napake, jih je potrebno čim prej odpraviti. Incidenti povezani s kriptografijo so skoraj zmeraj posledica »slabe« implementacije, nerazumevanja konceptov kriptografije in nepravilne uporabe. Znano dejstvo s področja varnosti je, da bo napadalec venomer poskušal razbiti najšibkejši člen, kar pa kriptografski algoritmi zagotovo niso.

LITERATURA

1. OWASP Guide to Cryptography, http://www.owasp.org/index.php/Guide_to_Cryptography, nazadnje obiskano 12.5.2010
2. OWASP, Cryptographic Storage Cheat Sheet, http://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet, nazadnje obiskano 12.5.2010
3. D. Goodin,'Severe' OpenSSL vulnerability busts public key crypto, The Register, http://www.theregister.co.uk/2010/03/04/severe_openssl_vulnerability/, nazadnje obiskano: 12.5.2010
4. A. Czeskis, D. J. St. Hilaire, K. Koscher, S. D. Gribble, T. Kohno, and B. Schneier, Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications, http://www.schneier.com/paper-truecrypt-dfs.pdf, nazadnje obiskano: 12.5.2010
5. Mögliche Schwachstelle in TrueCrypt 5.1, Heise Security, http://www.heise.de/security/meldung/Moegliche-Schwachstelle-in-TrueCrypt-5-1-190089.html , nazadnje obiskano: 12.5.2010
6. Tool zum Austricksen von Truecrypt veröffentlicht, Heise Security, http://www.heise.de/security/meldung/Tool-zum-Austricksen-von-Truecrypt-veroeffentlicht-832074.html, nazadnje obiskano: 12.5.2010
7. Data Encryption Standard (DES), NIST FIPS PUB 46-3, 1999, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf , nazadnje obiskano: 12.5.2010
8. Advanced Encryption Standard (AES), NIST FIPS PUB 197, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, nazadnje obiskano: 12.5.2010
9. N. Smart, *Cryptography: An Introduction*, MCGraw-Hill, 2003.
10. D. J. Barrett et al., SSH, the Secure Shell, Second Edition, O'Reilly, 2005.
11. S. Thomas, SSL and TLS Essentials, Wiley, 2000.
12. TrueCrypt - Free open-source disk encryption software, http://www.truecrypt.org/, nazadnje obiskano: 12.5.2010
13. Implementation Issues for Cryptography, NIST, http://csrc.nist.gov/publications/nistbul/csl96-08.txt, nazadnje obiskano: 12.5.2010
14. Block cipher modes of operation, Wikipedia, http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation, nazadnje obiskano: 12.5.2010
15. PKCS #5: Password-Based Cryptography Standard, RSA Laboratories, http://www.rsa.com/rsalabs/node.asp?id=2127, nazadnje obiskano: 12.5.2010
16. PHP blunders with random numbers, The H Open, http://www.h-online.com/open/news/item/PHP-blunders-with-random-numbers-967525.html, nazadnje obiskano: 12.5.2010
17. Windows-XP-Zufallszahlen ebenfalls zu schwach, Heise Security, http://www.heise.de/security/meldung/Windows-XP-Zufallszahlen-ebenfalls-zu-schwach-198634.html, nazadnje obiskano: 12.5.2010
18. OpenSSH vulnerability, Ubuntu Security Notice USN-612-2, 2008, http://www.ubuntu.com/usn/usn-612-2, nazadnje obiskano: 12.5.2010
19. Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), http://zakonodaja.gov.si/rpsi/r03/predpis_ZAKO1973.html, nazadnje obiskano: 12.5.2010
20. Session hijacking, http://en.wikipedia.org/wiki/Session_hijacking, nazadnje obiskano: 12.5.2010

SLOVENSKE SPLETNE APLIKACIJE IMAJO »TALENT«

Milan Gabor

ViRIS, Varnost in razvoj informacijskih sistemov
Inštitut za varnost podatkov in informacijskih sistemov
e-pošta: milan@viris.si
URL: http://www.viris.si/

Povzetek

Medtem ko se v Sloveniji iščejo talenti, lahko med spletnimi aplikacijami, ki jih najdemo na tudi na slovenskih straneh, najdemo različne talente. V prispevku bomo izpostavili tako dobre kot slabe prakse iz tega področja. Dotaknili se bomo tipičnih primeov in na njih prikazali, kako je mogoče z uporabo malo drugačnih talentov te aplikacije pripraviti, da nam povedo tisto, kar si avtorji definitivno niso želeli, da nam povedo. Hkrati bomo te naše talente primerjali s svetovno sceno in najbolj pogostimi napakami, ki jih lahko najdemo na OWASP seznamih. V prispevku bodo predstavljeni postopki in mehanizmi, kako se takšnih talentov znebiti.

1. UVOD

OWASP (Open Web Application Security Project) je odprta, globalna, brezplačna in neprofitna skupnost, ki se posveča dvigovanju varnostnega nivoja programske opreme. Poslanstvo OWASP je seznanjanje in osveščanje javnosti o pomembnosti aplikacijske varnosti in primernih načinih zavarovanja. V zadnjem letu se je začela ta skupnost prebujati tudi v Sloveniji in prvi rezultati se že začeli kazati. Glede na velik porast spletnih aplikacij v zadnjih letih, so se hkrati z aplikacijami začele množiti tudi potencialne varnostne pomanjkljivosti v teh aplikacijah. Vedno več aplikacij, ki so se iz intranetnih strani preselile na spletne strani in se s tem odprle širnemu svetu, so s sabo prinesle tudi veliko pomanjkljivosti. Zavedati se moramo, da razvijalci, ki so razvijali intranetne strani niso nikoli pomislili, da bodo te spletne strani kdaj dostopne tudi zunanjemu svetu in zato niso posvečali velike pozornosti varnosti v njih samih.

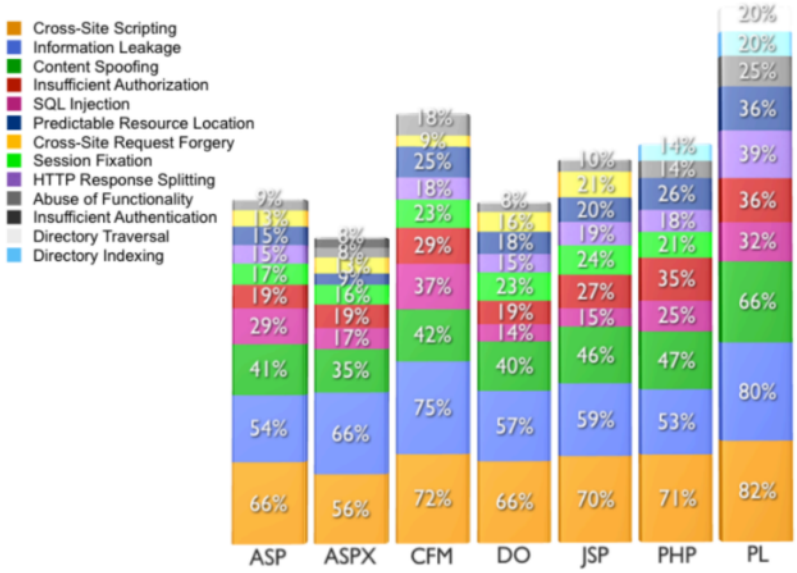
V generalnem za spletne aplikacije obstaja nekaj tipičnih napak in tudi OWASP pripravi vsake toliko časa seznam 10 najpogostejših napak. Takšen seznam je bil sestavljen nazadnje v letu 2007. V letošnjem letu so ga posodobili, tako da imamo čisto nov seznam desetih najpogostejših napak v spletnih aplikacijah. Če primerjamo seznam iz leta 2007 in 2010 lahko ugotovimo, da dejansko ni prišlo do večjih sprememb. Torej to pomeni, da v zadnjih treh letih dejansko ni bilo novih, večjih tipičnih napak, ki bi pristale na tem seznamu. Največja sprememba je na 10 mestu, kjer je pristala nova nevarnost, in sicer nepreverjene preusmeritve in posredovanja. Če pogledamo na hitro seznam napak pri vrhu, lahko ugotovimo, da so nekatere ranljivosti že kar stare, a so še vedno čisto pri vrhu. S tega lahko sklepamo, da tudi razvijalci še vedno delajo približno enake napake.

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross-Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross-Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	A8 – Failure to Restrict URL Access
A9 – Insecure Communications	A9 – Insufficient Transport Layer Protection
<not in T10 2007>	A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

Slika 1. Primerjava OWASP Top 10 ranljivosti iz leta 2007 in 2010

Poleg naših lastnih izkušenj lahko najdemo tudi zanimive rezultate v raziskavi [2], ki je analizirala preko 1500 spletnih aplikacij v časovnem razmaku od leta 2006 do začetka leta 2010.

Iz rezultatov navedene raziskave lahko vidimo, da so odstotki napak približno enako porazdeljeni po vseh programskih jezikih. Sicer so opažena nekatera odstopanja pri posameznih jezikih, a ta odstopanja niso velika. Iz rezultatov je moč razbrati, da napake, ki jih najdemo v aplikacijah niso odvisne od programskega jezika ali okolja v katerem so nastale, ampak so v veliki meri odvisne od izkušenosti razvijalcev. Če pogledamo širše in zunaj tega kontektsa, lahko opazimo, da se velika večina teh napak ponavlja in so klasične napake s seznama OWASP Top 10.



Slika 2. Rezultati analize [2] podjetja White Hat Security

2. TALENTIRANA APLIKACIJE V SLOVENIJI

Tudi za aplikacije, ki jih lahko najdemo na slovenskem spletu, lahko rečemo, da včasih pokažejo svoj »talent«. V ožji izbor je prišlo nekaj spletnih aplikacij, ki jih nekateri uporabljamo ali pa smo na njih naleteli naključno in v interakciji z njimi ugotovili, da so »talentirane«. Seveda pa bi jih lahko našteli še veliko več, saj lahko pri vsakodnevnem brskanju po Internetu najdemo veliko pomanjkljivosti v spletnih straneh. Pri odkritjih teh »talentiranih« aplikacij ni izjem glede tega, ali so bile poceni ali so stale malo premoženje in tudi ali so od garažnih podjetjih, ali pa za njimi stojijo močne ekipe razvijalcev. V nadaljevanju bomo na kratko prikazali »talent« nekaj aplikacij. Zaradi občutljivosti nekaterih podatkov pa vseh podrobnosti ne bomo izdali.

2.1 Razobličenja – »talent« nepravilne konfiguracije

Seveda se nam pogosto poraja vprašanje, kje »talente« iskat. Vemo da to ni enostavno delo, saj je potrebno dosti potrpežljivosti in iznajdljivosti, da najdemo res pravi talent. Ena vstopna točka je lahko tudi seznam razobličenih spletnih strani za domeno .si. Hekerji in ostali ki napadajo spletne strani, se radi pohvalijo glede njihovih dosežkov. Glede na to, da se pohvalijo kaj jim je uspelo in na kateri strani, so te spletne strani zelo dobri kandidati za naš izbor. Če pogledamo seznam za mesec marec letošnjega leta, lahko opazimo, da so poleg manjših spletnih strani nekatere označene tudi z zvezdico. Ta razobličenja imajo večjo vrednost kot ostala in če pogledamo so bile na seznamu tudi spletne strani Rdečega križa Slovenije in podjetja Bayer Pharme. Takšna mesta so torej idealen začetek zbiranja talentov. Izkaže se namreč, da poleg ranljivosti, ki so jih že izkoristili za razobličenja vsebujejo še kakšne druge pomanjkljivosti, ki so jih avtomatska orodja, ki jih uporabljajo, izpustila. Nekatera podjetja, ki jih je mogoče zaslediti na teh seznamih, smo tudi opozorili na te pomanjkljivosti, a so se na naš kontakt odzvali le redki.

Time	Notifier	H	M	R	★	Domain	OS	View
2010/03/16	KTN					www.malnaric.si/index.php/kmet...	Linux	mirror
2010/03/16	funky_still	H	M			www.offroadoprema.si	Linux	mirror
2010/03/16	Ghost_Rider		M			skywalker.si/forum/	Linux	mirror
2010/03/16	SQL@Live.se	H	M			psiholog.si	Linux	mirror
2010/03/12	KHG		M			suzuki.panjan.si/sl/predstavit...	FreeBSD	mirror
2010/03/12	KHG		M		★	www.rks.si/docs/	FreeBSD	mirror
2010/03/12	KHG		M		★	www.isuzu.si/f/	FreeBSD	mirror
2010/03/12	KHG		M			linuxdan.si/docs/index.htm	FreeBSD	mirror
2010/03/12	KHG		M			www.antivirus.si/docs/	FreeBSD	mirror
2010/03/12	1923Turk					tvojportal.si/jomtube/sploni-p...	Unknown	mirror
2010/03/11	1923Turk		M	R		www.simbioza.si/index/index.ph...	Linux	mirror
2010/03/10	funky_still	H	M			rozica.si	Linux	mirror
2010/03/10	funky_still	H	M			studio2010.si	Linux	mirror
2010/03/10	KHG		M			www.softnet.si/f/index.htm	FreeBSD	mirror
2010/03/10	KHG		M			www.ro.softnet.si/f/index.htm	FreeBSD	mirror
2010/03/10	KHG		M			www.cn.softnet.si/f/index.htm	FreeBSD	mirror
2010/03/10	KHG		M			www.rcl.si/f/docs/index.htm	FreeBSD	mirror
2010/03/09	KHG		M		★	bayerschering.bayer.si/docs/	FreeBSD	mirror
2010/03/09	khg		M		★	www.bayer-pharma.si/docs/	FreeBSD	mirror
2010/03/09	KHG		M		★	www.healthcare.bayer.si/docs/	FreeBSD	mirror
2010/03/09	Z7FaaN H4Ck3R					dat.si/publikacije	Linux	mirror
2010/03/09	KHG		M		★	www.bayer.si/docs/	FreeBSD	mirror
2010/03/09	KHG		M		★	www.thenorthface-slovenija.si/f/	FreeBSD	mirror
2010/03/09	KHG				★	www.suzuki.si/sl/predstavitev_...	FreeBSD	mirror
2010/03/09	KHG		M	R	★	www.suzuki-odar.si/sl/avtomobi...	FreeBSD	mirror

Slika 3. Seznam razobličenih strani za domeno .si

2.2 Spletni portal - talent nepreverjenega vnosa

Opis naslednje napake še ni bil popravljen, zato točnega naslova ne moremo izdati. Je pa zanimiva napaka in zato jo bomo opisali. Spletni portal, ki boleha za to napako, prenaša preko URLja zahtevke za id strani. Pri preverjanju smo opazili, da ta parameter ni problematičen, saj ni reagiral na standardne teste. Po naključju smo poskusili dodati na koncu id parametra še eno ničlo oz smo poskusili odpreti vnesti id, ki ni obstajal in tedaj se je stran začela odzivati precej počasi in nad rezultatom smo bili presenečeni celo sami. Aplikacija nam je namreč vrnila vsebino celotnega CMS sistema in v teh podatkih smo hkrati dobili ne samo vsebino spletne strani, ampak tudi podatke o prijavah vseh uporabnikov in tudi njihova gesla v kriptirani obliki. Tako talentiranih aplikacij, bi si želela večina hekerjev.

2.3 *.uni-mb.si - talent nepravilne konfiguracije

Pri brskanju po spletnih strani različnih organizacij v domeni uni-mb.si je možno naleteti tudi na zanimivo spletno aplikacijo, ki na primer ima že izpolnjene podatke o prijavi, torej uporabniško ime in geslo, saj je to precej olajšalo delo testnemu uporabniku. Po kliku na prijavo smo dobili naslednje sporočilo, ki ga ob pravilni konfiguraciji na noben način ne bi smeli. Še posebej zato ne, ker vsebuje tudi izpis kode in prikazuje privzete vrednosti ob določenem pogoju.

description The server encountered an internal error () that prevented it from fulfilling this request.

exception

```
org.apache.jasper.JasperException: An exception occurred processing JSP page /prijava.jsp at line 27

24:     aips.connect();
25:     //int status = 0;
26:     //PRAVA KODA
27:     int status = aips.veljaven(user, pass);
28:     if (user.equals("admin") && pass.equals("admin"))
29:     {
30:             session.putValue("student", "admin");


Stacktrace:
        org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:498)
        org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:411)
        org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:322)
        org.apache.jasper.servlet.JspServlet.service(JspServlet.java:249)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
        org.jboss.web.tomcat.filters.ReplyHeaderFilter.doFilter(ReplyHeaderFilter.java:96)
```

Slika 4. Napaka v spletni aplikaciji

2.4 Portal peljime.si - talent SQL vrivanja

Spletna stran www.peljime.si je precej nova in je pristala tudi na seznamu razobličenih strani in tako postala zanimiva za nas. Pri vnosu naslednjega URL naslova spletna stran deluje tako kot mora:

http://www.peljime.si/?lang=&option=content&podrocje=7&id=30.

Če pa le malenkost popravimo parameter področje, pa lahko vidimo, da nam spletna stran postreže z obilico podatkov o sami napaki in še drugih podatkih, ki so lahko še kako zelo koristni napadalcem. Tako smo lahko izvedeli cel SQL stavek, ki je uporabljen za povpraševanje, pot na disku, kjer so shranjene datoteke te spletne strani, dodatne spremenljivke in verzijo uporabljenega PHPja.

http://www.peljime.si/?lang=&option=content&podrocje=7a&id=30

NAPAKA

Sporocilo:	Pri SQL poizvedbi je prišlo do napake: Unknown column '7a' in 'where clause'
Datoteka:	/home/sinergija/domains/peljime.si/public_html/admin/classes/MySQL.php
Vrstica:	88
Sled napake:	

Datoteka:	/home/sinergija/domains/peljime.si/public_html/inc_left_menu.php
Vrstica:	33
Spremeljivke:	1 => SELECT t1.*, (COUNT(t2.content_id) - 1) AS depth FROM table_content AS t1, table_content AS t2 WHERE t1.lft BETWEEN t2.lft AND t2.rgt AND t1.lang='' AND t1.title!='root' AND t1.section_id=7a AND t1.state=1 GROUP BY t1.content_id ORDER BY t1.section_id, t1.lft
Datoteka:	/home/sinergija/domains/peljime.si/public_html/index.php
Vrstica:	247
Spremeljivke:	1 => /home/sinergija/domains/peljime.si/public_html/inc_left_menu.php

Datum in čas:	24.05.2010 ob 18:44:24
Okolje:	PHP 5.2.12 (Linux) na www.peljime.si

Slika 5. Prikaz napake na spletni strani

2.5 Svetovalka – talent nepreverjenega vnosa

Velikokrat naletimo na napake v spletnih aplikacijah, tam kjer dejansko pričakujemo, da jih ne bi smeli najti. Takšen primer je bil tudi primer eSvetovalke, ki so jo imeli na spletni strani občine Maribor. Pri predolgem vnosu se prikaže spodnja napaka, ki dejansko dosti pove o sami aplikaciji in njeni avtorici, ter izda še druge podatke, ki so lahko potencialnim napadalcem koristni.

Tako lahko na spodnjih slikah razberemo iz napake kje dejansko na disku se nahajajo spletne strani. Iz podatkov na drugi sliki pa lahko celo razberemo celo uporabniško ime avtorice eSvetovalke in pot na disku, kjer so bile izvorne datoteke.

Server Error in '/esvetovalkaUI' Application.

String or binary data would be truncated.
The statement has been terminated.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: String or binary data would be truncated.
The statement has been terminated.

Source Error:

```
Line 60:            //NEPRIMERNA VPRAŠANJA
Line 61:            NeprimernaVprasanja.NeprimernaVprasanja neprimernaV = new NeprimernaVprasanja.NeprimernaVprasanja();
Line 62:            odgovor = neprimernaV.PreveriVprasanje(posebneBesede);
Line 63:            odgovor = odgovor.Trim();
Line 64:
```

Source File: c:\AppRoot\ESvetovalkaMariborUI\App_Code\ESvetovalkaUIFunkcije.cs **Line:** 62

Slika 6. Prikaz napake na spletni strani

```
System.Data.SqlClient.SqlDataReader.ConsumeMetaData() +87
System.Data.SqlClient.SqlDataReader.get_MetaData() +112
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +2476580
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async)
+2478113
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method,
DbAsyncResult result) +424
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method) +28
System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +211
System.Data.SqlClient.SqlCommand.ExecuteDbDataReader(CommandBehavior behavior) +19
System.Data.Common.DbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) +19
System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable,
IDbCommand command, CommandBehavior behavior) +221
System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior
behavior) +573
System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable) +161
NeprimernaVprasanja.NeprimernaVprasanjaDL.PreveriPrimernostVprasanja(String stavek) in C:\Documents and Settings\Ines\My Documents\Visual Studio
2005\Projects\ESvetovalkaUI\NeprimernaVprasanja\NeprimernaVprasanjaDL.cs:31
NeprimernaVprasanja.NeprimernaVprasanjaBL.PreveriPrimernostVprasanja(String stavek) in C:\Documents and Settings\Ines\My Documents\Visual Studio
2005\Projects\ESvetovalkaUI\NeprimernaVprasanja\NeprimernaVprasanjaBL.cs:14
NeprimernaVprasanja.NeprimernaVprasanja.PreveriVprasanje(String vprasanje) in C:\Documents and Settings\Ines\My Documents\Visual Studio
2005\Projects\ESvetovalkaUI\NeprimernaVprasanja\NeprimernaVprasanja.cs:16
ESvetovalkaUIFunkcije.OdgovorNaVprasanje(String vprasanje, Int32 zapStVprasanja) in
c:\AppRoot\ESvetovalkaMariborUI\App_code\ESvetovalkaUIFunkcije.cs:62
_Default.Button1_Click(Object sender, EventArgs e) in c:\AppRoot\ESvetovalkaMariborUI\Default.aspx.cs:93
System.Web.UI.WebControls.Button.OnClick(EventArgs e) +115
System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +140
System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument) +29
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +2981
```

Slika 7. Prikaz napake na spletni strani

2.6 SIOL – XSS talent

Kot dokaz, da nimajo težave samo majhne spletne strani, lahko navedemo spletni portal moj.siol.net, ki je služil kot vstopna točka za nastavitve svojega računa. To ranljivost objavljamo zato, ker je bil ta prikaz prikazan že v eni izmed spletnih izdaj navodil za XSS napade. Ta XSS napad je bil objavljen sicer na tej spletni povezavi [3], ampak spletna stran trenutno ni dosegljiva, je pa zato še vedno mogoče priti do vsebine preko Google cache na tej povezavi [4].

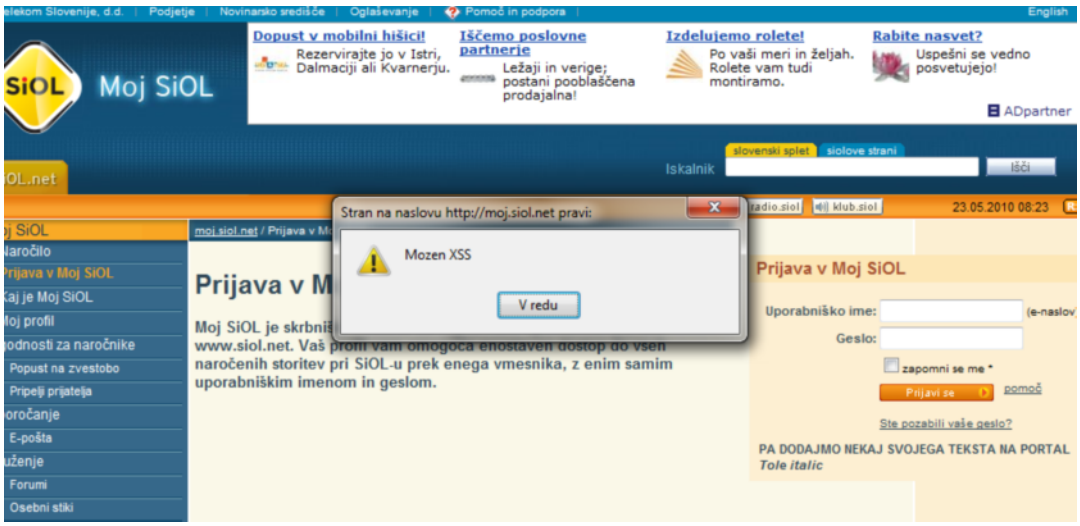
```
12.)
http://moj.siol.net/login.aspx?cams_login_failed=true&cams_login_config=http
&cams_original_url=http%3A%2F%2Fgoogle.com&cams_login_failed_message=%3Cimg%20
src=%22http://pointglow.com/dRake/mafioso.jpg%22%3E%3Cscript%3Ealert(%22lolz...
%20dRejk%20em%20aj%20;0%22)%3C/script%3E&cams_security_domain=system&cams_reason=7

http://moj.siol.net/login.aspx?cams_login_failed=true&cams_login_config=http
&cams_original_url=http%3A%2F%2Fgoogle.com&cams_login_failed_message=[XSS]
&cams_security_domain=system&cams_reason=7

- Da li je potrebno jovo nanovo objasnjavati i ovaj posebno ? :) Nema htmlspecialchars
niti bilo kakvog filtera...ccc ;p
```

Slika 8. Opis XSS luknje za moj.siol.net na hrvaški spletni strani

Z uporabo namiga z zgornje povezave, lahko v HTML kodo na strežniku vrinemo svoje tekste, HTML kodo ali celo javascript kodo. To smo v nadaljevanju tudi demonstrirali.

http://moj.siol.net/login.aspx?cams_login_failed=true&cams_login_config=http&cams_original_url=http%3A%2F%2Fgoogle.com&cams_login_failed_message=PA%20DODAJMO%20NEKAJ%20SVOJEGA%20TEKSTA%20NA%20PORTAL%3Cbr%3E%3CI%3ETole%20it

alic%3C/i%3E%3Cscript%3Ealert%28%22Mozen%20XSS%22%29%3C/script%3E&cams_security_domain=system&cams_reason=7



Slika 9. Primer XSS, ki s pomočjo javascripta odpre okno

Ker je SiOL spremenil prijavno stran na prijava.siol.net smo preverili, če je tudi na tej strani mogoča enaka napaka. Opaziti je bilo, da je možno po spletni strani pisati, ni pa več možno vpisovati javascripta ali drugih HTML oznak, saj je bila aktivirana zaščita, ki to onemogoča.

https://prijava.siol.net/default.aspx?cams_login_failed=true&cams_login_config=http&cams_original_url=http%3A%2F%2Fwww.siol.net&cams_login_failed_message=Tukaj%20je%20tekst%20na%20spletni%20strani&cams_security_domain=system&cams_reason=7

Slika 10. Dodajanje teksta na spletni strani prijava.siol.net

3. PRIPOROČILA »TALENTOM«

Veliko večino prikaza problemov »talentiranih« aplikacij je možno odpraviti v kratkem času z malo vloženega napora in tudi rešitve so precej enostavne za tiste, ki se s tem ukvarjajo. Predvsem je potrebna pravilna konfiguracija in sicer najprej samega okolja v katerem te spletne aplikacije potem tečejo, torej operacijskega sistema, PHP ali ASP okolja in same podatkovne baze. V velikem številu primerov je tudi opaziti, da je produkcijska aplikacija hkrati tudi razvojna ali testna aplikacija in se na njih dela tudi razvoj, kar lahko vodi do nepričakovanih rezultatov. Če bi nekako morali izbrati najpomembnejši nasvet pa je ta, da je potrebno vsak vnos, ki pride s strani uporabnika, preveriti. Ne moremo se namreč zanašati na to, da so uporabniki zanesljivi ali na primer, da se preverjanje vnosa opravi na strani uporabnika, saj se lahko ta preverjanja vnosov obide na enostaven in lahek način.

Vsa opažanja glede primerov aplikacij lahko strnemo v spodnje tri točke, s katerimi bi lahko »talentirane« aplikacije v veliki meri odpravili:

- opraviti je potrebno pravilno konfiguracijo programskega in sistemskega okolja,
- upoštevati je potrebno priporočila in dobre prakse pri implementaciji aplikacij,
- pred objavo spletne aplikacije je potrebno interno ali eksterno preveriti aplikacijo glede pravilnih nastavitev in varnosti.

4. ZAKLJUČEK

V prispevku smo prikazali, da tudi v Sloveniji obstaja veliko »talentiranih« ljubiteljskih in tudi profesionalnih razvijalcev, ter posledično tudi kar nekaj »talentiranih« aplikacij. Dokler so te aplikacije namenjene samo spletnim predstavitvam ni težav. Težave se lahko pokažejo, ko te aplikacije začnejo prenašati kakšne osebne podatke ali druge občutljive podatke. Veliko neželenih »talentov« lahko tako predstavlja potencialno veliko nevarnost ne samo za podatke, ampak tudi za informacijske sisteme, ki so zgrajeni okrog teh spletnih aplikacij. Kot vemo je Internet dinamična stvar in prav tako tudi napadalci, zato je mogoče včasih priporočljivo poseči tudi po zunanjih izvajalcih, ki lahko pomagajo zmanjšati število »talentiranih« aplikacij.

LITERATURA

21. *http://www.owasp.org/*,
    OWASP *Top 10 2010*.

22. *WhiteHat Website Security Statistic Report,Spring 2010, 9th Edition, www.whitehatsec.com, 2010*.

23. XSS SIOL
    http://presszone.org/home.pz?misc=search&subaction=showfull&id=1263128230&archive=&cnshow=news&start_from=&ucat=3

24. Google cache: http://webcache.googleusercontent.com/search?q=cache:E7d-jGzcgusJ:presszone.org/home.pz%3Fmisc%3Dsearch%26subaction%3Dshowfull%26id%3D1263128230%26archive%3D%26cnshow%3Dnews%26start_from%3D%26ucat%3D3+xss+moj.siol.net&cd=7&hl=sl&ct=clnk&gl=si&client=firefox-a

"Race condition" - Ko želva stavi na srečo, zajec pa na "symlink" napad

Jure Škofič

Acros d.o.o.
e-pošta: jure.skofic@acrossecurity.com
URL: http://www.acrossecurity.com

Povzetek

Članek obravnava ranljivosti tipa »tekmovalni pojav« (ang. »race condition«), natančneje za podskupino TOCTTOU (»time of check to time of use«). Do ranljivosti te vrste prihaja zaradi neatomarnosti operacij preverjanja obstoja ter odpiranja/kreiranja datotečnih objektov. Cilj napada je ponavadi proces, ki teče s korenskimi privilegiji in datotečni objekti, ki jih proces uporablja. Uspešnost izkoriščanja tekmovalnih pojavov je odvisna od mnogih faktorjev in tako daje vtis naključnosti in nezanesljivosti. V tem članku bom demonstriral tehniko, ki omogoča zanesljivo izkoriščanje omenjenih ranljivosti.

1. UVOD

Pogosta praksa razvijalcev je kreiranje začasnih, lahko tudi izvedljivih datotek v direktorijih, ki so dostopni vsem (npr. /tmp, /var/tmp). Ker za delo s temi datotekami uporabljajo neatomarne (večkoračne) operacije, postanejo aplikacije ranljive za ranljivosti tipa »tekmovalni pojav«. Uspešnost takega napada pa ob uporabi prave tehnike ni nikakršna loterija. Ranljivost tekmovalnega pojava v kombinaciji s tehniko »symlink« labirinta omogoča zanesljivo izvedbo napada, katerega posledice lahko segajo od izvajanja sovražne kode v kontekstu procesa ter dviga privilegijev (»elevation of privileges«) do napadov odrekanja strežbe (»denial of service«).

2. IZKORIŠČANJE TOCTTOU TEKMOVALNIH POJAVOV

2.1 Tekmovalni pojavi

Tekmovalni pojav nastopi, ko dva ali več procesov ali niti dela s skupnimi viri. Taki viri so lahko datoteke, skupni pomnilniški objekti ipd. V informacijski varnosti pa za tekmovalni pojav smatramo akcijo, ko proces preverja neko stanje (recimo obstoj datoteke) in na podlagi tega izvede akcijo, stanje pa se lahko med tem spremeni. Takó stanje ob času preverjanja (»time of check«) ni enako stanju ob uporabi (»time of use«). Takšnim tekmovalnim pojavom pravimo TOCTTOU tekmovalni pojavi (»time of check to time of use«).

2.2 TOCTTOU ranljivosti na LINUX datotečnih sistemih

TOCTTOU ranljivosti so zelo razširjene in dobro znane in se pojavljajo na datotečnih sistemih s šibko sinhronizacijsko semantiko. Eden izmed takih je tudi Linux datotečni sistem.

Na operacijskem sistemu Linux obstaja okrog 220 parov sistemskih klicev [1], ki se uporabljajo za preverjanje stanj in izvajanja akcij na podlagi teh stanj. Ob pogoju, da je objekt dostopen napadalcu, je vsak tak par je ranljiv za TOCTTOU.

Med pogosteje uporabljenimi pari sistemskih klicev tako najdemo:

- <stat,open>
- <stat,chmod>
- <stat,mkdir>
- <open,chmod>
- <open,chown>
- <open,open>
- <mkdir,chmod>

Na Linux operacijskem sistemu obstaja veliko direktorijev, ki so imuni na tovrstne napade (Tabela 1), saj napadalcu zaradi dobre konfiguracije pravic dostopa onemogočajo vpogled, pisanje v datoteke ali kreiranje datotečnih objektov.

/bin	/mnt	/usr/etc	/usr/sbin	/var/ftp
/boot	/opt	/usr/include	/usr/src	/var/lock
/dev	/root	/usr/lib	/usr/X11R6	/var/log
/etc	/proc	/usr/dict	/var/cache	/var/lib
/lib	/sbin	/usr/kerberos	/var/db	/var/run
/misc	/usr/bin	/usr/libexec	/var/empty	

Tabela 1: Direktoriji, imuni na TOCTTOU napade[1]

Pogosta praksa razvijalcev pa je kreiranje datotek v začasnih direktorijih (npr /tmp). Takšne datoteke so lahko med drugim tudi izvedljivi skripti (npr. Makefile). Razvijalec preveri, če takšna datoteka že obstaja, preden jo kreira, vendar naredi usodno napako: za kreiranje datoteke uporabi klic open() z zastavico O_CREAT, pozabi pa na zastavico O_EXCL, ki vrne napako, če datoteka že obstaja. To omogoča napadalcu, da med klicem, ki preverja obstoj datoteke, in klicem open() v direktoriju kreira datoteko z istim imenom. Če proces nato te datoteke ne kreira, temveč jo odpre in vanjo piše, ima napadalec lastništvo nad datoteko. Tako jo lahko uporabi v svoje namene.

```
If(stat("/tmp/datoteka") == -1)
{
        open("/tmp/datoteka", O_CREAT)
        //V datoteko zapiše bash skript

}
.
.
.
execve("/tmp/datoteka")
```

Slika 1: Primer ranljive kode

2.3 Primer TOCTTOU tekmovalnega pojava

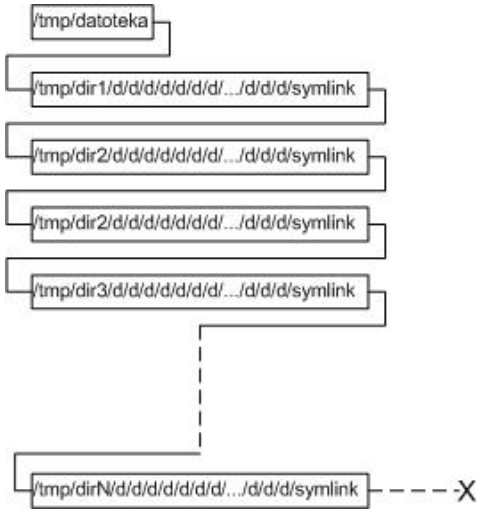
Eno izmed slabše dokumentiranih ranljivosti tipa TOCTTOU najdemo tudi v paketnem upravljalcu Rpm. Ko Rpm namešča ali odstranjuje programe, v direktoriju /var/tmp/ kreira »bash« skript, ki skrbi za nameščanje ali odstranjevanje dokumentacije. Rpm v tem primeru uporabi par klicev <open, open>, kjer s prvim klicem open() kreira datoteko in vanjo zapiše kodo, z drugim pa datoteko odpre in jo izvede. Ker datoteko kreira s pravicami dostopa, ki vsakomur omogočajo pravico pisanja (666), lahko napadalec po prvem klicu v datoteko zapiše sovražno kodo, ki jo nato Rpm izvrši. Ta ranljivost se smatra za kritično, saj se ponavadi programi nameščajo in odstranjujejo s korenskimi privilegiji.

2.4 Izkoriščanje ranljivosti TOCTTOU s pomočjo »symlink« labirintov

Običajno pa napadi na TOCTTOU ranljivosti niso tako trivialni kot zgoraj omenjena ranljivost. V omenjenem primeru med obema klicema open() preteče veliko časa, kar napadalcu omogoča, da z večjo verjetnostjo pridobi procesorsko časovno rezino in izvede napad ob pravem trenutku. V večini primerov ranljivosti TOCTTOU pa je časovno okno mnogo manjše. Ponavadi gre za dva zaporedna klica, kar daje napadalcu izredno malo časa, da izvede napad. V tem primeru pa lahko napadalec uporabi tehniko, ki mu omogoča sinhronizacijo z napadenim procesom in pridobitev procesorske časovne rezine ob pravem času.

Omenjena tehnika se imenuje »*symlink labirint*« in izkorišča razliko v zmogljivosti procesorja in trdega diska. »Symlink« ali *simbolična povezava* je datoteka, ki vsebuje le referenco na drugo datoteko. Vse operacije, ki jih izvajamo nad simbolično povezavo, se odražajo na datoteki, na katero se sklicuje simbolična povezava. Prav tako lahko ustvarjamo »symlink« z neobstoječo referenco. Ti dejstvi napadalcu omogočata uspešno izvedbo napada.

Za primer vzemimo kodo s slike 1. Da napadalec uspešno izvede napad, mora datoteko ustvariti med klicem stat() in klicem open(). Njegov prvi cilj je sinhronizacija z napadenim procesom, ki jo doseže tako, da kreira »symlink« z imenom »napadene« datoteke, ki nima reference. Ko proces na simbolični povezavi izvede klic stat(), ta vrne vrednost -1, saj referenca ne obstaja, hkrati pa spremeni čas dostopa na »symlinku«. Napadalec lahko spremembo časa dostopa periodično preverja s klicem lstat(), ki pa »symlinku« ne spremeni časa dostopa. Tako lahko zanesljivo ve, da je bil nad »symlinkom« izveden klic stat() s strani napadenega procesa. Na tej točki mora napadalec pridobiti procesorsko časovno rezino, da lahko simbolično povezavo odstrani in na njenem mestu podtakne svojo (sovražno) datoteko.



Slika 2: Symlink labirint

Procesorsko časovno rezino napadalec pridobi s pomočjo »symlink labirinta« (Slika 2). Labirint je sestavljen iz verige simboličnih povezav, gnezdenih v direktorijih, in tako prisili jedro operacijskega sistema, da razreši celotno verigo, preden proces ugotovi, da datoteka ne obstaja - to da napadalcu dovolj časa za izvedbo napada.

Za lažjo predstavo, zakaj je ta operacija tako časovno zahtevna, zapišimo nekaj pomembnih dejstev o ext3, enem najpopularnejših datotečnih sistemov operacijskega sistema Linux,:

- Vsak datotečni objekt je velik vsaj 4 kB.
- Največja dolžina poti, ki jo jedro lahko obravnava, je 4 kB.
- Največja globina »symlinkov«, ki jih lahko povežemo v verigo, je 40.

Napadalec lahko tako ustvari labirint, ki vsebuje okoli 80.000 direktorijev, ti direktoriji pa zavzemajo 327 MB prostora na disku. Kreiranje labirinta sicer povzroči, da se le-ta shrani v predpomnilnik, vendar ga lahko od tam tudi odstranimo. To lahko storimo z zagonom iskanja datotek po disku ali pa ustvarimo še kak labirint, ki prvega izrine iz predpomnilnika.

Tovrstni labirinti so možni tudi na mnogih drugih Unix operacijskih sistemih, le da se razlikujejo v maksimalni dolžini in velikosti (tabela 2).

Operacijski sistem	**Datotečni sistem**	**Maksimalna dolžina poti**	**Maksimalna dolžina symlink verige**	**Velikost direktorija (kB)**	**Maksimalna dolžina labirinta**	**Maksimalna velikost labirinta (MB)**
Linux 2.6.8	Ext3	4.096	40	4	81.920	327
Solaris 9	Ufs	1.024	20	0,5	10.240	5
FreeBSD 4.10-PR2	Ufs	1.024	32	0,5	16.384	8

Tabela 2: Velikosti labirintov na različnih operacijskih in datotečnih sistemih [2]

Pri tako veliki količini podatkov je zelo verjetno, da vsaj enega direktorija ne bo v predpomnilniku, kar prisili jedro operacijskega sistema, da med izvajanjem klica stat() začne brati s trdega diska in med tem prekine njegovo izvajanje. Napadalec tako dobi procesorsko časovno rezino, odstrani prvi »symlink« v verigi in na njegovem mestu ustvari datoteko. Ko jedro razreši labirint, ugotovi, da zadnji »symlink« v verigi nima reference in tako kaže »v

prazno«. Sistemski klic stat() vrne -1, napadeni proces pa začne izvajati klic open(), ki odpre napadalčevo datoteko in vanjo zapiše skript. Ker pa ima napadalec lastništvo nad to datoteko, lahko v skript podtakne sovražno kodo in s tem povzroči, da se njegova koda izvede v kontekstu napadenega procesa.

2.5 Zaščita pred tovrstnimi napadi

Najboljša zaščita je seveda osveščenost. Če razvijalec obvlada pisanje varne kode, se zna tekmovalnim pojavom tudi izogniti. V opisanem primeru bi bilo najbolje uporabiti klic open() z zastavico O_EXCL. Ta zastavica bi zagotovila, da datoteke ne bi bilo mogoče podtakniti, saj bi klic vrnil napako. V našem primeru bi namesto izvajanja kode prišlo samo do ranljivosti odrekanja strežbe ("denial of service"). Določeno zaščito nudijo tudi naključna imena datotek, kar pa omejuje pogosta predvidljivost uporabljenih psevdo-naključnih generatorjev števil. Predvsem pa se je potrebno izogniti lokacijam, ki so prosto dostopne vsem. S kombinacijo teh protiukrepov se lahko učinkovito ubranimo pred tovrstnimi napadi.

3. ZAKLJUČEK

Operacijski sistem Linux dosega le kakšen odstotek tržnega deleža vseh operacijskih sistemov, zato je v njem znanih veliko manj varnostnih napak kot v sistemih Windows. To pa še zdaleč ne pomeni, da je ranljivosti malo. Kljub temu, da »race condition« napadi občasno zahtevajo lokalni dostop, so lahko posledice v kombinaciji s kakšno drugo ranljivostjo, ki omogoča oddaljen dostop, katastrofalne. Iskanje tekmovalnih pojavov na datotečnem sistemu je za izkušenega strokovnjaka zelo preprosto, saj Linux nudi vsa potrebna orodja in večinoma celo možnost vpogleda v izvorno kodo. Zato ko boste naslednjič pisali aplikacijo, se spomnite vsaj tega, da pospravljanje datotek v direktorij /tmp pač ni najboljša izbira in da želva v tekmi z zajcem le težko zmaga.

LITERATURA

25. *TOCTTOU Vulnerabilities in UNIX-Style File Systems: An Anatomical Study*: Jinpeng Wei and Calton Pu, Georgia Institute of Technology, 2005.

26. *Fixing Races for Fun and Profit: How to abuse atime:* Nikita Borisov Rob Johnson Naveen Sastry David Wagner, University of California, Berkeley, 2005.

TELESNI SKENERJI NA SLOVENSKIH LETALIŠČIH

Edvard Šilc

e-posta: edvard.silc@guest.arnes.si

Povzetek

V zadnjem času opažamo poplavo tehničnih pomagal s katerimi naj bi zagotavljali večjo varnost v poslovnih okoljih. Večja varnost je glede na pretnje nujno potrebna, vendar verjetno ne na rovaš ostalih človekovih pravic. Pri uvajanju teh pomagal se lahko dogodi, da so v nasprotju z integriteto posameznika. Pravica posameznika je pri nas natančno regulirana in sankcionirana.

Nacionalno varnost kot najvišjo obliko varnosti, pogosto zagotavljamo na račun drugih človekovih pravic, saj se v tem primeru prilagodijo tudi pravne norme. V svojem prispevku sem opisal primer uvajanja telesnih skenerjev na letališčih, ki eksplicitno znižujejo pravico do zasebnosti in po poglobljeni analizi vidimo, da ne zagotavljajo večje varnosti. Namen obveznega nakupa teh naprav na evropskih letališčih je le profit proizvajalca, dobaviteljev in drugih v posel vpletenih ljudi.

1. UVOD

Na IDC roadshowu o varnosti smo slišali novo izhodišče, ki je zanimivo za IT: »Varnost je kot letališče.« To izhodišče pomeni, da moramo na varnost v poslovnih sistemih gledati, kot na varnostne izzive na letališčih, z neomejeno možnostjo vdorov različnih oblik in intenzivnosti[1].

S tem prispevkom, kot poseben izziv, želim prikazati oblikovanje potreb po varnosti na letališčih, ki so odziv na različne oblike terorističnih dejanj[2].

1. *IDC IT Security, Virtualization and Datacenter Roafdshow 2010, 11.05.2010, Ljubljana, Predavanje Notranji varnostni pregled - Naslednji korak zagotavljanje varnosti, mag. Borut Žnidar Astec d.o.o. in predavanje predstavnika ISACA mag Janka Uratnika.*

2. *Terorizem je organizirano nasilno dejanje, ki je usmerjeno proti civilnemu prebivalstvu in sledi politični ali gospodarski ciljem. Terorizem je večinoma na očeh javnosti, saj teroristi želijo čim večjo odzivnost v medijih. Na ta način oblikujejo javno mnenje k svojim ciljem.*

   Zgodovina terorizma Pojem *terorizem izhaja iz zaključka francoske revolucije leta 1793 in 94, ko so javno pobijali pripadnike revolucionarnih odborov. Kasneje se je s tem pojmom označevalo nasilje države nad prebivalstvom z obsojanjem na giljotiranje.*

Dejanja, ki so značilna za teroriste so bila po doktrini Sveta za zunanje zadeve ZDA izvajana že od pradavnine. S tem nazivom so poimenovani tudi sveti bojevniki, ki so pobijali civiliste, kot so judovski fundamentalisti, ki so pobijali Rimljane, kot prebivalce Palestine okrog leta 100.

Moderne oblike terorizma *so prilagojene široki svetovni populaciji prejemnikov informacij iz »mainstream« medijev. Za prvenec teh dejanj smatramo ugrabitev komercialnega potniškega letala julija 1968, ki ga je izvedla Ljudska fronta za osvoboditev Palestine.*

V zagotavljanju višje varnosti na nivoju posamezne države ali skupnosti držav, kot je Evropska unija ali zveza NATO, se oblikuje tudi nacionalna ali nadnacionalna varnostna politika. Z globalizacijo je vsaka državna varnostna politika in njeno izvajanje del varnostne politike sveta, čeprav se po drugi strani še vedno zaznava, da imamo na tem polju bolj vplivne države, velesile ali skupnosti držav, kjer se oblikujejo elementarni pogoji za ohranitev relativnega svetovnega miru. Globalizacija varnostnih politik se kaže tudi v finančnih interesih dobaviteljev varnostnih rešitev, oborožitve in podpornih sistemov. Po mojih spoznanjih že vse od priprav na ameriško državljansko vojno in Napoleonovim zavzetjem večjega dela Evrope in tudi naših krajev po letu 1800 (sama državljanska vojna je trajala od 12.04.1861 do 9.04.1865) lahko potrdim tezo, da je nacionalna varnost v povezavi z velikimi finančnimi vložki in profiti. Posledično s tem pa tudi z različnimi interesi, lobiji in vplivi, ki želijo sooblikovati vse oblike varnostne politike. Kljub temu, da gre za izjemno občutljiva vprašanja nacionalne in nadnacionalne varnosti, zasebni interesi vnašajo velike deviacije, ki pogosto pripeljejo v gospodarske in politične razprtije ali celo oboroženih spopadov. Ob pomanjkanju zaupanja, stvarnih dokazov ali neoporečnih prič o vlogah ob implementacijah varnostnih rešitev, se pojavijo različna izhodišča, ki jih pogosto imenujemo kar teorije zarot. Teorije zarote skuša uradna politika prikazati kot nekaj nerealnega, izmišljenega, zavajočega in škodljivega za javni interes, kljub tem zagotovilom se po daljšem času izkaže kakšno takšno izhodišča za verjetno in izvedljivo. V političnem marketingu teorije zarot prispevajo svoj delež k uspehu ali porazu določene politične opcije, zato jih politika s pridom uporablja kot politično orožje za dosego partikularnih interesov [Southwell 2004, 415 in 416].

Na primeru uvajanja telesnih skenerjev, si bomo v nadaljevanju ogledali način uvajanja visoke tehnološke rešitve, ki naj bi zagotovila večjo varnost na letališčih, letalih in urbanih okoljih, ki so cilji napadov teroristov z ugrabljenimi letali. Obljube o večji varnosti, zaradi izkušenj v preteklosti, sprožijo diskurz pri posameznikih, civilnih iniciativah in v mnogih primerih celo pri uradni politiki, ki opozarja, da gre la za novo omejevanje človekovih pravic, kot so pravice do osebne varnosti, pravice do zasebnosti, pravico javnosti, da je obveščena, pravica do zagotavljanja zdravja in druge [Šinkovec 1997, 52].
Skeniranje telesa je tehnologija pregledovanja, ki omogoča vpogled pod oblačila. To pomeni, da se s tem načinom ne posega le v polje človekove zasebnosti (polje osebnega delovanja) temveč v polje posameznikove intime, torej v polje intimnega delovanja [Šinkovec 1997, 43].

Slika1: prikazuje različne nivoje delovanja posameznika v interakciji s socialnim okoljem. Pri tem je vsak posameznik v lastnem središču vseh svojih koncentričnih kvadratov ali krogov. Intimno področje je metaforično vezano na spalnico in kopalnico, v nekaterih primerih tudi na zdravniške preglede in posege. To področje je torej v popolni domeni

posameznika in se javni interes tu ne sme in ne more vsiljevati.
Skeniranja temeljijo na rentgenski oziroma radioaktivni tehnologiji. Različne oblike sevanja, ki so s tem povzročene, škodijo predvsem zdravju oseb, ki so v nenehnem stiku z skenerjem. V mnogo manjši, vendar zaenkrat neznani, meri pa so pod vplivom teh žarčenj tudi potniki, ki jih na ta način pregledujejo. Ta vpliv narašča s pogostostjo in številom posegov preverjanja s skenerji. Med nivoje varnosti posameznika sodi tudi zdravstveno varstvo, kjer naj bi veljalo medicinsko načelo, da je bolje preprečevati kot zdraviti. Problem nastane tudi zaradi tega, ker pravih podatkov o teh žarčenjih ni. Vsaka stran jih tako lahko prireja svojim potrebam. Nasprotniki trdijo, da telesni skenerji bistveno povečujejo možnost rakavih obolenj, zagovorniki pa trdijo, da je ta vpliv minimalen oziroma zanemarljiv.

Tudi pred uvedbo skenerjev za telesni pregled potnikov, so na letališčih pred poletom, opravili vrsto kontrol. Najbolj sporno, za večino potnikov, je sezuvanje čevljev in kontrola pijač. Uvedba telesnih skenerjev bi bila morda za potnike manj nevšečna, če bi z njeno uvedbo odpadle druge oblike kontrole. Na letališčih, kjer so telesne skenerje uvedli, še vedno izvajajo kontrolo pijač, ki jo lahko vnesemo v letalo in potniki se morajo še vedno sezuvati čevlje[3].

3. Pravila o vnosu tekočin oziroma omejitvi vnos tekočin v letala veljajo na podlagi Uredbe Evropske komisije in začasnem soglasju Evropskega parlamenta, ki si zelo prizadeva to uredbo umakniti. Uredba valja od 06.11.2006, na vseh letališčih v EU ter tudi na Norveškem, v Islandiji in Švici. Pravila so se uveljavila po poizkusu terorističnega napada na letalo s tekočim eksplozivom, ki letijo med Veliko Britanijo in ZDA avgusta 2006.

Po tej odredbi lahko potniki na varovano območje letališča in v letalo vzamejo le tekočine v embalaži, ki ne sme biti večja od sto mililitrov (1 deciliter). Plastenko ali stekleničko morajo hraniti v prozorni plastični vrečki katere prostornina ne presega tisoč mililitrov, oziroma enega litra. Ta vrečka se mora zapreti. V primeru da potnik tekočino pokaže na več kontrolah in jo vmes uporablja, mora biti vrečka prilagojena za vodo-tesno večkratno zapiranje.

Omejitev velja za vse vrste tekočin, kot so pijače, juhe, sirupi in tudi za gele, paste (tudi krema za čiščenje ali izpiranje zob, šampon za umivanje las, tekoče milo), olja in losjone, parfume, razpršilce (tudi dezodoranti, pene za britje, črtala za trepalnice)... Izjeme veljajo samo za tiste tekočine, ki se med potovanjem uporabljajo iz zdravstvenih razlogov ali zaradi specifičnih zahtev prehrane in tekočine oziroma predmete, ki jih potniki kupijo ali dobijo na nadzorovanem delu letališča ali na varnostnem območju omejenega gibanja.

Za lažji nadzor izvajanja te uredbe morajo potniki pri kontroli:

- *pokazati vse (v prejšnjem odstavku) opisane tekočine, ki sodijo v ročno prtljago potnika. Najprimernejši način za to je, da potniki vrečke s tekočinami prenaša ločeno izven svoje osebne prtljage ali posebnem predalu osebne prtljage,*
- *pred pregledom varnostnika morajo sleči gornje vrhnje oblačilo, kot je to na primer suknjič, jopič ali plašč, ki se pregleduje ločeno,*
- *iz ročne prtljage morajo potniki izločiti prenosne računalnike in druge večje električne naprave, ki se pregledujejo ločeno.*

Pravila ne veljajo za tekočine, ki jih potniki hranijo v oddani prtljagi. V ročni prtljagi so lahko tudi zdravila in nujno potrebna živila, vključno z otroško hrano, ki se jemljejo med potovanjem. Za dovoljen prenos lahko pri pregledu zahtevajo tudi *ustrezno pojasnilo (potrdilo o jemanju zdravil, karton za sladkorne bolnike, ki jemljejo zdravila ali si dajejo inzulinske injekcije in otrok, ki potrebuje otroško hrano).*

Vse vrste tekočin, ki so ustrezno zapakirane že ob nakupu na področju letališč, ki so se dolžna ravnati po tej odredbi, morajo biti ob pregledu varnostnika v originalni embalaži. V takšnem primeru lahko količina tudi presega predpisano, vendar ob dejstvu, da se mora tekočina nahajati v neodprti embalaži in zaprti vrečki. Če je embalaža že odprta jo lahko pri pregledu izločijo.

Z javno polemiko, ki jo izvajajo civilne, nevladne in provladne institucije, in se vodi hkrati z uvajanjem teh naprav, se je dosegel dogovor, da pregled opravljajo različne osebe, po fizično ločenih in medsebojno oddaljenih prostorih, da se zmanjša možnost zlorabe. To pomeni, da oseba, ki dela s telesnim skenerjem ne vidi slike na ekranu, ker se ta prenese k osebi, ki je izven dosega pogleda na to osebo. Na ta način naj bi se omejila možnost zlorabe zaposlenih, ki izvajajo nadzor na letališčih (v tem tekstu varnostniki)[4].

2. DILEMA

Za poglobljen diskurz o terorističnih dejanjih, ki so se začela z napadom 11. septembra 2001 v ZDA in so pripeljala do različnih incidentov, spopadov in celo vojn, imamo kot državljani premalo verodostojnih podatkov. Večinoma so v te dogodke vpletene različne strani, ki prikazujejo dogajanja vsaka po svoji meri. Na osnovi teh nedorečenih in težko dokazljivih dejanj temeljijo tudi nacionalne in nadnacionalne varnostne politike. Hkrati z njimi pa se sooblikujejo različne teorije zarot, ki vzpodbujajo razmišljanja o drugi obliki interesov in motivov za povzročene incidente [Southwell 2004, 10 in 11 ter Gordon 2002, 49, 105].

Po 11.09.2001 se je oblikovalo stališče, da je varnost posameznika in družbe najpomembnejši dejavnik, četudi na škodo ostalim človekovim pravicam. V obdobju po zrušitvi Newyorških dvojčkov, je bil gnev posameznikov napram napadalcem tako močan, da je vse kazalo na to, da bo družbena klima pristala na takšno izhodišče. S časom so se zahteve po večji varnosti ponovno začele usklajevati z drugimi človekovimi pravicami. Precej sta k tej paradigmi prispevala tudi podjetji HP in IBM z objavo, da sta v njihovih rešitvah varnost in zasebnost enakovredno zastopana in soodvisna.

Naslednje obdobje, kjer se je zvišala zahtevnost po varnosti tudi na področju Evropske unije je bilo po napadu na Madrid 11.03.2004. Sledil je napad v Londonu 07.07.2005. Zadnji primer pa je poskus napada v Detroitu konec lanskega leta. Vsako od teh obdobij je prineslo vrsto sprememb k varnosti in kasneje tudi nasprotno reakcijo, ko so z zakonskimi in drugimi predpisi skušali ublažiti rigidnost varnostnih zahtev napram drugim človekovim pravicam.

Uspelo teroristično dejanje vpliva na vsakega posameznika z osebnimi odzivi in strokovnimi odločitvami na različnih področjih dela in delovanja. V IKT smo varnost posvojili kot pomemben sestavni del delovanja in povezovanja funkcij v instituciji kjer delujemo. Tako skrbnejše izdelujemo varnostne kopije, te kopijo hranimo na več medijih in več lokacijah, ki bi bile v primeru naravne nesreče ali incidenta izven področja delovanja, imamo tudi rezervne lokacije, ki bi prevzele delo primarne lokacije po incidentu. Od naših uporabnikov zahtevamo, da spremenijo načine vedenja in dela, ki zagotavljajo večjo varnost, zapisujemo potek dogodkov in dejanj, ki bi preprečili izgubo podatkov ob incidentu in skušamo zagotoviti celostno varnostno politiko tudi z implementacijo preverjenih standardov na tem področju. Opravljamo tudi simulacije napadov, penetracijske teste in druge varovalne ukrepe. Skrbno

merimo, načrtujemo in beležimo okrevanje po incidentu. Izobražujemo vse zaposlene, uravnavamo organizacijski model in odgovornosti, pregledujemo log zapise, kontroliramo podvojene, potrojene zapise, odstranjujemo nepotrebne in nedovoljene zapise (osebne podatke po obdobju rabe) in podobno, vse za večjo varnost naših IT in poslovnih sistemov.

4. *Strahovi pred vdori v zasebnost so se že realizirali tudi v praksi. Po poročanju Žurnala 24, naj bi zaposleni na letališču komentiral golo podobo iz ekrana skenerja svoje sodelavke v izmeni, ki je nehote stopila v prostor, kjer se skeniranje izvaja.*

Povečan nivo varnosti prestavlja za vsako poslovno okolje večje stroške, ki jih vsakdo poskuša vgraditi v prodajni produkt ali storitev. Konflikt z usmeritvijo nižanjem stroškov je tako neizbežen že v lastnem poslovnem okolju z argumenti, da se primerljiva teroristična dejanja kot v ZDA, Veliki Britaniji, Španiji v Sloveniji ne bodo ponovila. K skepticizmu o nivoju varnostne zaščite svoje prispevajo tudi povsem upravičeni diskurzi o teoriji zarot, kar lahko zniža pričakovane kriterije varnosti v naših poslovnih okoljih.

Višji nivo varnosti ne zahteva le večjih finančnih vložkov in implementacije na novo pridobljenih (kupljenih) ali posodobljenih rešitev, pač pa posega tudi v druge že uveljavljene načine življenja posameznika in skupin. Zdi se, da večja varnost omejuje druge človekove pravice in povečuje nadzor. Ob tem se večkrat pojavijo tudi izhodišča, da je temu potrebno prilagoditi tudi temeljne listine države kot so to mednarodne pogodbe, evropski pravni red, ustavo in abstraktne zakone.

V sami dilemi sem odprl vrsto vprašanj na katere ni enostavnih odgovorov. Nanje lahko od različnih ljudi dobimo vrsto pojasnil, ki se kmalu zopet preoblikujejo v enaka vprašanja, ker prvotna pojasnila ne prinašajo verodostojnih dokazov. Vse te dvome si bomo približali ob dogodkih izpred nekaj mesecev, ki so kalili praznovanje prehoda v letošnje koledarsko leto.

2.1 Dogodki na božični večer

Na osnovi prebranih tekstov v medijih in s sklepanjem na osnovi znanih dejstev, bi lahko za incident napisal zanimiv in verjetno napet scenarij. Morda beseda scenarij ni ustrezna, ker vzpodbuja razmislek o predlogi za snemanje filma, ne glede na namen (komercialni, dokumentarni, propagandni film). Ta termin sem navedel predvsem za to, da bomo lažje oblikovali različne možnosti, sklepanja in sosledja.

Dejstvo je, da se je nigerijski državljan Umar Farouk Abdulmutallab 24.12.2009 vkrcal na letalo letalske družbe Nortwest, ki je letelo od Amsterdama do Detroita. Nimamo poročila o tem kako mu je uspelo priti mimo letališke kontrole, ker je:

- imel pri sebi kemično snov v tekoči obliki, ki se ne sme vnašati na letala,
- je bil na spisku domnevnih teroristov ali njihovih sodelavcev.

Lahko pa domnevamo, da je letališka kontrola zaradi velikega števila ljudi v stavbah pred letališčem popustila v budnosti ali pa so bili varnostniki zaradi prazničnega obdobja manj

pazljivi. Morda je manjkalo nekaj zaposlenih ljudi in so ostali ob misli, da bi bili raje v okolju svojih družin in prijateljev, svoje delo opravljali manj skrbno kot sicer. To je le domneva!

Kasneje so v nekaj poskusih novinarji dokazovali, da je kemično snov ali drugo tekočino možno prenesti mimo kontrole na letališču, s telesnim skenerjem, tudi če se pregledovalec drži predpisanih postopkov. Ravno tako, ni mogoče po istem viru preveriti vse potnike, če se slučajno ne pojavljajo na kakšnih spiskih domnevnih teroristov. Na spisku na katerem je bil Umar je bilo še 550.000 drugih imen. Ob tem se pojavi vprašanje čemu po tem služijo ti spiski imen in ali sodobna tehnologija res ni v stanju preveriti takega spiska v nekaj sekundah s spiskom potnikov za določeno letalo in sprožiti alarm, če pride do usklajenosti.

Pred dogodki, ki jih je povzročil Umar Farouk Abdulmutallab me je znanec, ki ima zaradi prometnih prekrškov večkrat opravek s Policijo, povprašal o principu delovanju naši mož v modrem. Vprašanje je bilo povezano z njegovo izkušnjo, ko je na osebni avto namestil kar registrske tablice drugega (kombiniranega) vozila. Ta znanec živi v primestnem okolju, kjer se nizajo družinske hiše in bi takšno okolje po ogroženosti lahko opredelili kot mirno področje z nizko kriminaliteto. Nasprotno temu pa je njegovo delovno okolje, ki ga sestavlja nepregledna množica na novo nastalih stanovanjskih objektov, s težje kontroliranimi migracijskimi tokovi, črnimi gradnjami in nastanitvami, kjer se pričakuje višja stopnja kriminalitete. Vozilo je uporabljal za prevoz iz enega okolja v drugo, kar je opravil nekajkrat na dan, ker ima doma skladišče za vrednejše materiale. Drugi dan popoldne, takšnega nelegalnega prevoza, ga je odkrila policijska patrulja, ki se je s službenim vozilom vozila po cesti. Vprašanje, ki je sledilo je bilo: »Kakšen princip ima sedaj Policija, da lahko tako hitro reagira«, posebno ob njegovem zagotovilu, da se je pred petimi leti tako vozil cel mesec in ni imel nobenih težav. Iz vseh dodatnih spoznanj, ki vplivajo na moj odgovor domnevam, da ima Policija tehnologijo, ki ne temelji le na policistovi intuiciji, preverjanju registrske tablice po radijski zvezi s centrom za informiranje in reagiranju, če je povratna informacija drugačna kot je stanje, ki ga policist opaža na cesti. Torej domnevam, da ne gre samo za vizualizacijo, ker je šlo za neproblematično vozilo, kabriolet starejšega letnika, ki ga bi lahko uvrstili med ljubiteljska vozila in kot taka ne povzročajo incidentov.

Če je moja domneva pravilna in se izvaja avtomatsko branje registrskih tablic, preverjanja v zbirki registriranih vozil in opozorilo v primeru neskladja podatkov, bi tak sistem preprečeval, da bi sedaj nekdo opravljal prevozniško obrt tako, da bi imel na tovornjaku registrske tablice iz svojega osebnega vozila, kot se je to lahko dogajalo pred leti. V primeru, da je moja domneva pravilna (policistov o tem seveda nisem spraševal, ker bi jih spravljal v zadrego) lahko upravičeno pričakujemo, da se tak način uvede na letališčih, seveda z izhodiščem iz IT, da mora biti podatkovna zbirka ustrezna in se tako prepreči princip »smeti noter smeti ven«.

Umar (v tem tekstu to ni kratica za Urad za makroekonomske analize in razvoj) se je na letalo vkrcal z lastnimi verodostojnimi dokumenti. Postavi se vprašanje, kaj bi pomenilo za varnostni sistem, če bi bili dokumenti (v celoti ali delno) ponarejeni? Na letalo, se je poleg domnevnega terorista, vkrcalo še 277 potnikov in članov posadke. Zakaj se je Umar vkrcal ravno na to letalo v tem času? Ali je bilo to poglobljeno načrtovano? Z veliko gotovostjo bi lahko potrdili takšno tezo. Če so teroristi želeli povzročiti čim več škode, je bil let in čas ustrezen. Nismo pa prišli do odgovora kako poglobljena je bila priprava na to dejanje s strani teroristov. Še vedno obstoja domneva, da je Umar deloval v manjši skupini, čeprav je sam povedal da dela za Osamo Bin Ladna. Tudi odgovornost za ta napad je prevzela mednarodna

teroristična organizacija Al Kaida, ki je preko arabske televizije Al Džezira sporočila: »ZDA ne bodo niti sanjale o varnosti, dokler ne bodo varni Palestinci, ki jih ogroža Izrael!«

Domnevamo tudi, da je terorist pretihotapil kemično snov mimo kontrol na letališču v svojem telesu. Za to snov domnevamo, da je bilo tekoče razstrelivo, ki ob vžigu povzroči visoke temperature, se ne da pogasiti z vodo in lahko v ustreznih razmerjih eksplodira. Voda je celo medij za prenos, če se razlije skupaj s pomešanim eksplozivom. Tega skener ne odkrije.

Ali je Umar med letom letala iz Amsterdama priti Detroitu pritegnil kakšno pozornost s svojimi ravnanji? Domnevamo ne! Pred pristankom letala v avtomobilsko mesto je Umar Farouk Abdulmutallab, po navedbah prič iz tega letala, izlil po tleh tekočino v tistem predelu potniškega dela letala, ki je nad eklektičnimi vodniki in to razlito snov poskušal zažgati z vžigalnikom. Očitno se je terorist premikal po potniški kabini iz predela, kjer je prej sedel in s tem morda pritegnil določeno pozornost, čeprav se pred pristankom nemir pri potnikih povečuje in se nekateri težje zadržijo na svojih sedežih. Ob teh navedbah je lahko veliko skepse. Velika verjetnost je, da bi moral terorist tik pred dejstvom zmes šele pripraviti, v ustreznem razmerju, o čemer pa ni nobenega zapisa.

Vžiganje z vžigalnikom tekočine na tleh (ali po drugih virih še vedno v vedno steklenici) je pritegnilo pozornost, kajti pri tem delu je bil terorist očitno nespreten, saj so ga mnogi potniki iz letala lahko opazovali. Posebno priseben naj bi, po objavljenih dejstvih, bil potnik Jasper Schuring, ki je skočil proti nigerijskemu napadalcu, ga odrinil, mu iz rok iztrgal vžigalnik in omejil začetni požar. Kasneje je policistom povedal, da je bil ugrabitelj letala povsem odsoten, neagresiven in vdan v svojo usodo, tako da ga je zato z lahkoto obvladal. Pri tem dejanju naj bi rešitelja Jasperja Schuringa vodil le nagon za ohranitev svojega življenja in življenja drugih potnikov, saj naj ne bi bil za takšna dejanja posebej usposobljen[5].

5. *Prva uradno zabeležena ugrabitev letala (po angleško hijackings) se je dogodila v Peruju 21.02.1931. Domneva se, da je dogajanje potekalo po naslednjem zaporedju. Pilota Byrona Rickardsa so revolucionarji zajeli na letališču Arequipa. Po tem, ko so že imeli pilota, so si prilastili še letalo znamke Ford s tremi propelerskimi motorji. Namen te ugrabitve z razliko od kasnejših je bil, da bi ugrabljeno letalo uporabljali za prevoze svojih ljudi in materiala. Pilot je ukaze revolucionarjev o poletih zavrnil. Po deset dnevnih mirovanja letala, prepričevanja in pogajanj, ko so revolucionarji v svojem gibanju uspeli, so pilota zamenjali za zajetega revolucionarja. Sama zamenjava je bila v Limi.*

   Po drugi svetovni vojni je število ugrabljenih letal strmo naraslo. V letih (oziroma desetletju) med 1948 in 1957, je bilo ugrabljenih 15 letal. V desetletju med 1958 in 1967, se je število povečalo na 48. Naslednje revolucionarno leto 1968, se je število ugrabitev povečalo na 38 in leta 1969 so beležili rekord s kar 82 ugrabitev. Rekordno je tudi desetletje od leta 1968 do leta 1977, ko je bilo ugrabljenih kar 414. Temu obdobju je sledilo povezovanje držav kjer so bila letala registrirana z državami, kjer so ugrabljena letala največkrat pristajala. Tak sporazum je bil za časa druge Nixonove administracije podpisan s Kubo in Kitajsko. ZDA so vplivale tudi na Izrael, ki je za to izboljšal svoje mednarodne odnose z Egiptom, Jordanijo in Palestinsko osvobodilno organizacijo Jaserja Arafata, ki se je odpovedala podpori teroristom. Jaser Arafat je pot začel kot revolucionar, danes bi rekli terorist-strokovnjak za razstreliva in peklenske stroje.

Dogovor o ne podpori ugrabiteljem je velja tudi ves čas pogajanj med PLO in Izraelom. Državam, ki z ZDA niso hotele imeti prijateljskih odnosov je ameriška administracija zagrozila s sankcijami. Primer sta Libija in Sirija. Velik upad ugrabitev je povzročil tudi umik iz aktivnega delovanja frakcij rdečih armade v Italiji in (Zahodni) Nemčiji.

Pomembno je tudi dejstvo, da se je zelo povečalo tudi število in obseg varnostnih ukrepov in pregledov na civilnih letališčih. Število ugrabitev letal je tako v naslednjih desetletjih upadlo na povprečno 18 na leto.

V povojnem obdobju je bila večina ugrabitev zaradi odkupnin za letalo, člane posadke in potnike. Piloti so večinoma opravljali svoje delo po navodilih ugrabiteljev, drugi člani posadke pa so morali sedeti s potniki in čakali na razplet. Ugrabitelji so skušali ohraniti življenja ugrabljencev in svoja življenja. Kasneje so ugrabitelji tudi pilotirali, vendar je bilo takih primerov pred 11.09.2001 zelo malo. V tem obdobju se zato že pojavijo tudi obrambni načrti, ki temeljijo na sestrelitvi ugrabljenega letala. Jasno je, da so ti načrti povzročili veliko negodovanja med državljani potencialnimi potniki in žrtvami.

Po 11. septembru 2001 se je položaj zelo spremenil. Celotna posadka in potniki so postali talci. Ugrabitelji so za dosego postavljenega cilja žrtvovali svoja življenja in življenja potnikov in članov posadke. Posledica tega je, da se načrtuje aktivni upor potnikov in članov posadke. Člane posadke tako sedaj urijo tudi za proti teroristično delovanje. Piloti sporočajo dogovorjen znak 7500, kar pomeni, da je letalo ugrabljeno, oziroma znak 7600, da je izgubljeno zaradi prevzema pilotskega dela s strani druge posadka. Vrata v pilotsko kabino so sedaj okrepljena. Morebitni vlom teh prehodnih vrat se registrira v nadzornem centru. Predvideva se tudi možnost prevzema daljinskega nadzora letenja letala iz nadzornega centra, če bi bilo letalo ugrabljeno. Še vedno nekatere države zagovarjajo sestrelitev ugrabljenega letala. Ta izredno težavna odločitev nosi šifro 9/11. Tak ukrep so v Indiji uzakonili. Podobno so ravnali v Nemčiji, vendar je zvezno ustavno sodišče ta zakon razveljavilo. Pravno ureditev akcij teroristov nad civilnimi letali urejata tudi dve mednarodni konvenciji. To sta Haaška in Montrealska konvencija.

V boju proti kakršni koli nevarnosti, ki nastopi se praviloma uspešnejše po robu postavi tista oseba, ki je dejanje predvidela in pri tem ustrezno orodje ali celo orožje ni najpomembnejši faktor. Mnoge institucije, ki usposabljajo organe pregona (vojska, policija, varnostno obveščevalne službe, enote obrambe in zaščite) pri urjenju gradijo na dejstvu, da je uspeh določene (napadalne ali obrambne) akcije odvisen predvsem od pripravljenosti na pravilno reakcijo udeleženih ljudi in ne toliko na ustreznost in količino orožja. Drugače povedano najsodobnejše orožje v rokah osebe, ki jo popade panika, negotovost ali nemoč, ne pomeni prav dosti. Ob nekontroliranem vzpodbujanju (drugih oseb ali zavedanja da nekaj mora ukreniti) lahko pride celo še do večjih napak in težav. V trenirani osebi se sproži ustrezen postopek, ki ni povsem razumsko naravnan. Pogosto se uveljavlja princip posega ob elementih agresije, kar poveča adrenalin in hitrost in jakost ravnanja.

Ob tem se odpira še vrsto dejstev, ki izhajajo iz stališča, da lahko vrhunsko pripravljena oseba za proti teroristična ali drugačna varnostna ali borbena dejanja, v stvarni situaciji povsem odpove, čeprav je urjenje končala z nadpovprečnimi uspehi in se nekdo, ki je bil ne teh urjenjih povsem povprečen, v stvarni situaciji povsem drugače odreže. O tem je bilo mnogo napisanega a v stvarni situaciji tovrstna teorija ne pomeni mnogo. Tudi raziskave osebnosti niso korelirale s posamičnimi v praksi izkazanimi primeri.

Za moja razmišljanja je oseba, ki je rešila potnike pred terorističnim dejanjem na letalu Nortwesta največja uganka. Kdo je Jasper Schuring? Odgovori, ki jih je posredovala policija v Detroitu, po opisanem incidentu, so prikrojene informacije službe za stike z javnostjo, ki naj bi pomirila državljane, predvsem pa potencialne letalske potnike.

Ali je bil Jasper Schuring usposobljen za varnostno dejanje kor policist, vojak, varnostnik? Ali bi v njegovem psihološkem profilu lahko našli netipična dejstva? Kakšen človek, bi bil še

ustrezen za naš scenarij in bi mu hkrati zaupali dejanje, ki ga je izvedel? Dejanje je naredil popolnoma sam, brez podpore drugih potnikov, spontano, dovolj hitro, da je bilo tudi učinkovito. Prav gotovo je to edina dobra praksa v celotnem dogajanju.

Ali se je pred poletom pojavil kakršen koli indic o potencialni nevarnosti terorističnega napada in so letalske družbe na letala poslale tudi specialiste za obvladovanje teroristov? Tudi, če vnesemo to dejstvo v scenarij, bi bila njegova naloga predvsem kot »oficirja za vezo« ali pogajalca, manj pa v obvladanju terorista, ki lahko dejanja izvaja povsem nekontrolirano, ker mu pri tem nista mar osebna varnost ali življenje. Domneva, da bi dejanje terorista lažje uspelo kaže na to, da ni bilo ciljne skupino napadenih, ker med potniki ni bilo pomembnih osebnosti. Edini cilj so bile ZDA in tu povzročena velika škoda med človeškimi žrtvami.

Ali bi lahko oseba, ki povsem odstopa od zapisanih domnev, torej ni »programirana« za obvladovanje teroristov, na božični večer, ko je vse v pričakovanju prijetnih izkušenj, zbrala dovolj poguma in brez pomisleka zaščitila lastno življenje in življenja mnogih nedolžnih žrtev z aktivnim posegom v dogajanje? V primeru, da se pogledam v ogledalo, moram priznati, da jaz takšna oseba nisem, čeprav so me od srednje šole dalje učili, da je življenje borba.

Ker sooblikujemo scenarij, se lahko ozremo v filmske vode in ugotovimo, da tudi, če je Jasper Schuring mojster borilnih veščin ali če ima zmožnost adrenalinske kulminacije kot je menda to značilno za agresivne športe (na primer hokejiste), bi se težko odločil za akcijo, ki jih za velike in male ekrane pripravijo sodobni filmski junaki kot so Jean Claude Van Damme, Steven Segal ali Michael Dudikoff kjer ustrezne posnetek dobimo s serijo poizkusov pred kamerami in željo nasprotne strani da ga junak obvlada. Najmanj, kar bi pomisli je dejstvo, da ima terorist pri sebi strelno orožje. Jasper pa je akcijo opravil povsem brez oborožitve.

V tekstu sem zapisal, da je edini primer dobre prakse poseg Jasperja Schuringa, čeprav je seveda srečni konec vreden presoje, ki je ni bilo. Ob vseh znanih dejstvih, da je terorist s kemičnimi pripravki vstopil v letalo, mino predpisanega varnostnega pregleda, ki je na mednarodnem letališču v Amsterdamu še posebno natančno določen, kasnejša preiskava postopkov preverjanja potnikov ni pokazala napak.

Ta primer se je zahvaljujoč prisebnosti potnika rešil ugodno za prebivalce več milijonskega avtomobilskega mesta, potnike in člane posadke letala. Izkušnja, ki je bila s tem pridobljena je vsaj po medijskih informacijah ostala nezaznavna in sam dogodek je bil aktualen le za to, da bi se ponovno vzpodbudile razprave o povečanih varnostnih ukrepih pri pregledih potnikov na letališčih pred vkrcanjem na letala. Verjetno pa sam scenarij (za to smo ga tudi tako imenovali) v drugih situacijah ni izvedljiv, ker ni pričakovati, da bi se terorist, ki namerava storiti tako obsežno in pogubno dejanje, tako zlahka vdal. Ni tudi pričakovati, da bi se posredovanje ene osebe (tudi če je bil specialec na letalu) tako ugodno razpletlo. Tudi tu se tako pojavi dvom o zapisanem zaporedju dogodkov, oziroma je na delu teorija zarote.

Nekaj dni po tem, ko smo zakoračili v novo leto, se je navidezno, kot posledica teh dogodkov odvijalo srečanje »notranjih ministrov« članic držav, ki so povezane v Evropsko unijo.

2. 2 Posvet v Toledu

Na posvet ministrov za notranje zadeve EU o nujnosti zagotovitve večje varnosti na letališčih, boju proti terorizmu in s tem povezane teme o uvedbi pregledovanja na letališčih EU s telesnimi skenerji, so bili povabljeni vsi ministri za notranje zadeve (ali pravosodje, če sta

resorja prepletena) članic EU. Posvet je bil 21. 01. 2010 v Španskem mestu Toledo. S strani Slovenije, oziroma našega Ministrstva za notranje zadeve, se je tega posveta udeležil državni sekretar na Ministrstvu za notranje zadeve g. Goran Klemenčič, ki mu zadnje čase novinarji napovedujejo odhod z ministrstva, menda zaradi neskladja z ministrico Katarino Kresal.

Gorana Klemenčiča v vlogi namestnika ministrice Kresalove, s posebnim zanimanjem spremlja vsa slovenska strokovna javnost, že vse od njegovega imenovanja. Znana so namreč njegova radikalna stališča za zaščito zasebnosti in drugih človekovih pravic, ki jih je kot predavatelj na Fakulteti za varnostne vede (prej Visoki policijski varnostni šoli) širil z gorečnostjo zaščitnika civilne pobude, ki mora paziti le na točnost svojih radikalnih izjav. Državnemu sekretarju, ki menja ministrico, na tako pomembnem sestanku, pa načel revolucionarnosti borca za človekove pravice, ne moremo in niti ne smemo pripisovati.

K izhodišču omejitve nastopa na sestanku v Toledu dodajmo tudi slovensko prislovično majhnost (oportunizem in konformizem), ko se je potrebno sprejeti radikalne ukrepe, ki jih priporočajo organi EU na pobudo starejših članic unije ali ZDA. Na konferenco v Toledu je prišla namreč tudi ameriška državna sekretarka za domovinsko varnost Janet Napolitano, kar je še dodatno segrevalo zimsko politično ozračje. Sedaj lahko zapišem, da je Napolitanova na konferenci želela boljšo pozicijo za varnost ZDA, doseči le z nazornim opisovanjem dogodka v Detroitu, oziroma pred njim in ni postavljala pogojev ameriške administracije o nalogah EU za večjo varnost v svetu (tudi to bi bila za politiko legitimna dejanja, ki jih ne smemo očitati).
Na tej konferenci so bila dana naslednja izhodišča v razpravah o uvedbi in uporabi telesnih skenerjev (body scanner):

1. Povzročitelj incidenta v Detroitu je priznal, da deluje za mednarodno teroristično organizacija Al Kaida. To je »potrdila« tudi arabska televizija Al Džezira s prenosom izjave Osame Bin Ladna, ki je prevzel odgovornost za to dejanje.

2. Imamo tehnologijo, ki lahko zagotovi večjo varnost v zračnem prometu. To izhodišče je poudarjal predvsem italijanski notranji minister. To tehnologijo je po mnenju pristašev potrebno uporabiti na vseh letališčih EU, ki so vključena v sistem ene kontrolne vstopne točke (One stop control). Pri tem se je uporabilo kot argument tudi izhodišče, da je veriga tako trdna kot je močan najšibkejši člen. V EU so nekatere države ogrožene bolj in druge manj. Pomislek za nas je predvsem v tem, da Slovenija spada med manj ogrožene države, saj je edini teroristični napadalec hrvaški veteran Josip Zagajski, prispel k nam z vlakom.

3. V kleteh bruseljskih oziroma strasbourških vladnih palač, so po nekaterih navedbah ti skenerji že na zalogi, ker so bili kupljeni pred približno dvema letoma. Po (tihem) mnenju evropskih birokratov, je potrebno to tehnologijo le implementirati v državah članicah in se bodo rešili starih zalog. Cene telesnega skenerja je približno 100.000 (dolarjev ali evrov), poleg tega je potrebno znesku dodati tudi stroške montaže, ker je potrebno povečati prehode na gabarite skenerjev. Ti so mnogo večji kod naprave, s katerimi so do sedaj preverjale potnike z magnetnimi opozorilniki prisotnosti kovin in njihovo osebno prtljago z rentgensko napravo za pregled vsebine. Zaradi redundance bi morali imeti vsako letališče najmanj dva telesna skenerja.

Med prisotnimi na konferenci v Toledu, je bilo tudi mnogo skeptikov in nasprotnikov nujnosti uvedbe pregledovanja potnikov na tak način. Ti so imeli vrsto protiargumentov, ki jih lahko strnemo v dve naslednji točki:

1. Potnika med pregledom skenerji praktično »slečejo do golega« in s tem posegajo v

njegovo dostojanstvo, ugled in pravico do zasebnosti. Posebno problematično in sporno bi bilo, če bi pregledovalec (varnostnik) te slike posredoval medijem ali pa jih prenesel na splet z zapisom kateri osebi slika pripada.

2. Skenerji povzročajo sevanje, ki je lahko rakotvorno in zdravju škodljivo. Po določeni statistični verjetnosti naj bi vsak tisoč dvestoti potnik prejel takšne doze žarkov, da bi to bistveno znižalo odpornost proti rakastim obolenjem.

Med vsemi stališči za in proti, je bila prisotna dilema o tem ali bi pri Umarju Farouku Abdulmutallabu našli nevarne snovi, ki jih je preko mejne kontrole mednarodnega letališča v Amsterdamu, pretihotapil skrite v spodnjicah, v katere je bil oblečen. Zagovorniki skeniranja so trdili, da bi nevarne snovi skener zaznal, nasprotniki pa seveda povsem drugače.

Nastalo dilemo je skušal pojasniti tudi profesor Gruber s soočenjem na nemški televiziji in s kasnejšimi posnetki te oddaje na spletu, ki so bili aktualizirani v slovenski civilni iniciativi za zaščito zasebnosti aktualni, v času vikenda po konferenci od 22. do 24. januarja 2010. Prevod razgovora s profesorjem Gruberjem je v naslednjem poglavju tega teksta.

Dan kasneje so soočili svoja mnenja o konferenci in smiselnosti uvajanja telesnih skenerjev mag. Goran Klemenčič, dr. Ciril Ribičič iz pravne fakultete, dr. Iztok Prezelj iz obramboslovja FDV, Dušan Sofrič iz ljubljanskega letališča. Njihove poglede bi skrčil v naslednje točke:

1. Konferenca v Toledu, zaradi različnih pogledov med predstavniki držav EU, ni dosegla ustreznega konsenza, ker so bila stališča med zagovorniki uvedbe skenerjev (predstavniki Nizozemske, Anglije, Italije,…) in nasprotnikov uvedbe (predstavnikov Nemčije, Španije, Češke, Slovenije) povsem različna. Najtežje so zagovorniki oporekali predstavniku Španije, ki je bila žrtev terorističnega napada in tako je tudi odpadel očitek naši državi in Češki, da lahko odklanjamo skenerje, ker nismo bili še žrtev terorizma.

2. Razlogi izpred dveh let, ko je Evropski parlament že ustavil namen Evropske komisije, ki je takrat želela uvesti skenerje, se kljub poskusu napada na letalo, ki je letelo nad Detroitom niso bistveno spremenili. Še vedno je nedorečeno vprašanje ali skenerji res predstavljajo ustrezno varnostno rešitev.

3. Po sprejemu Lizbonske pogodbe, ni več zagotovljena avtonomija notranjega pravnega reda države članice EU, oziroma nima posamezna država članica več suverenost nad svojimi notranjimi zadevami, kot so to do sprejema pogodbe dovoljevale pravice iz prvih dveh stebrov. S to pogodbo se je pravica odločanja o notranjih zadevah posameznih držav, ki so v skupnem pomenu, prenesla na organe EU. Tako sedaj o uvedbi skenerjev odločajo v Svetu ministrov za promet. Očitno je, da so s sestankom v Toledu »potipali teren«.

4. Ves čas je prisoten občutek, da bi države članice EU uvedle obvezno skeniranje na zahtevo ZDA. Torej bi ta postopek uvedli predvsem zaradi varnostih zahtev v Ameriki in ne toliko za varnost v Evropi.

5. Dosedanji varnostni ukrepi na letališčih EU zahtevajo višje finančne vložke. Dejstvo je, da se del tega zneska prevali na potnike, del na davkoplačevalce, del pa na lastnike in zaposlene na letališčih. Ta strošek povečuje skupne stroške, ki jih letališče ima za 10.000 do 50.000 evrov na teden, v odvisnosti od že uvedene tehnologije in velikosti letališča.

Poleg tega pa se zaradi varnostnih ukrepov znižuje tudi pretočnost potnikov, ki se je že sedaj, ko nimajo vsa letališča skenerjev zniža za 30 do 60 odstotkov. To pomeni tudi zamude letal in s tem večjo nevarnost v zraku, ki se reflektira tudi na večjem številu napak letališkega in letalskega osebja.

6. Invazivnost teh naprav ni natančno opredeljena. Zagovorniki in nasprotniki so tu zelo različnih mnenj in pogledov. Prav gotovo, pa so te naprave bolj škodljive človeku kot ročno pregledovanje ali naprave, ki odkrivajo le prisotnost kovin.

7. Telesni skenerji po vseh dosedanjih spoznanjih ne odkrivajo:
   - tekočin
   - praškov ali snovi z minimalno granulacijo (torej tudi ne nove organske plastike)
   - tankih plastičnih predmetov
   - vse materiale s podobno strukturo kot jo ima človeško telo (koža)
   - vse kar je skrito v človekovem telesu (ustih in ostalih odprtinah).

8. Pogovori o uvedbi dodatnih varnostnih naprav se ne smejo opravljati po incidentu, ker v takšnem primeru prevladajo čustva, ki ne vodijo k najboljšim rešitvam. Za odločitev je potrebna določena časovna distanca, ko pridobimo relevantne podatke. Po incidentu so zagovorniki uvedbe skenerjev navajali število dejanj, s področja mednarodnega terorizma, ki se dogodijo vsako leto. Število je 400-600, kar vpliva na presojo. Z retencijo teh podatkov vidimo, da so zabeleženi tudi dogodki, ki bi jih težko enačili z incidenti, čeprav je incident po pojmovanju IT varnosti vse kar se dogodi in ni predpisano (Janko Uratnik)[1].

   Med incidente se uvrščajo tudi grožnje iz pisem ali forumov, ki so uperjeni proti bivšemu predsedniku ZDA. Tak primer imamo tudi pri nas, ko je Georgu Bushu pisal Slovenec iz Prekmurja in mu, po navedbi ameriških preiskovalnih organov, v pismu grozil.

9. V času po incidentu smo slišali tudi grožnje, da bo ZDA dovolila le pristanek tistim letalom, ki so letala z letališč, ki imajo skenerje. Sedaj, ko je imelo in še vedno ima, civilno letalstvo vrsto težav zaradi krize, stavk in prizemlitve letal zaradi islandskega vulkanskega pepela, si kaj takega nihče več ne upa napovedovati.

Evropska unija mora tovrsten probleme reševati skupaj s konsenzom svojih članic. ZDA so doživele pretnjo nevarnost iz zraka. Za to bi morali v Evropi uvesti skenerje. V Slovenijo se je edini terorist hrvaški bombaš Josip Zagajski pripeljal z vlakom. Ali bo EU zato na vseh železniških postajah uvedla pregled potnikov? Najbrž ne!

Ostaja tudi vprašanje smiselnosti projekta SWIFT in Terrorist finance tracking program. Pri SWIFT gre vsaka mednarodna finančna transakcija skozi center v Bruslju, TFTP je program, ki so ga naredili v ZDA in naj bi z njim nadzirali finančne transakcije v Evropi.

2.3 Zaključek poglavja

Osnovna teza je bila ali bomo tudi pri nas morali kupiti telesne skenerje. Mislim, da ne, ker je proti predlogu o nujnosti njihove uvedbe na vseh letališčih v EU, tudi evropski parlament. Njegovi poslanci so podvomili v pozitivni prispevek teh naprav. Koordinator EU za boj proti terorizmu Gilles de Kerchove je poslancem v odboru za državljanske svoboščine dejal: »Ti skenerji se bodo lahko uporabljali, ko bodo spoštovali zasebnost in bodo zdravju prijazni«.

O tem vprašanju so že razpravljali tudi na odboru za promet EU. Predsednik Brian Simpson je dejal, da si želimo optimalni nivo varnosti, vključno z varnostjo osnovnih človekovih pravic. »Ljudje, ki verjamejo, da so telesni skenerji pravi odgovor, si zatiskajo oči pred stvarnostjo.«

Seveda pa je vrsta lobistov in prodajalcev, ki vztrajajo pri svojem. Ti so prepričani, da so skenerji nujnost. Ti signali prihajajo predvsem iz ZDA, kjer telesne skenerje tudi izdelujejo.

Vprašanje je seveda tudi, kaj so se v ZDA naučili ob zadnjem dejanju terorista, ko so na Times Squareu našli terenski avto z eksplozivnimi snovmi. Spomnimo se, da so (po viru STA, Dnevnik in Večer) Ameriški policisti 03.05.2010 aretirali 30-letnega Faisala Shahzada, ameriškega državljana pakistanskega rodu, ki je priznal, da je pripravil ponesrečen teroristični napad 1.5.2010 v New Yorku. Terorist je skoraj ušel iz ZDA, kljub temu da je bilo tudi njegovo ime na seznam oseb, ki imajo povezavo s teroristi. Policisti so ga tik pred vzletom, prestregli na letalu za Dubaj in naprej proti Istambulu. Shahzad je po aretaciji priznal, da je skušal izvesti napad. Terorističnih veščin se je učil v pakistanski pokrajini Vaziristan, kjer imajo oblast talibani in teroristična mreža Al Kaida.

Med terorističnim poizkusom na Detroit in konferenco v Toledu, so v studiu nemške televizije gostili profesorja Gruberja, ki je dokazoval s primeri, pred kamerami zamajal zaupanje v telesno skeniranje. Pri prikazu je uporabljal eksploziv Termit, lahko pa bi imel druge spojine V naslednjem poglavju opisujem dejstva in pogovore s te oddaje.

3. VAJA PROFESORJA GRUBERJA

V filmu se odvija dialog med voditeljem oddaje in prof. Gruberjem, gospodom Haskettom, ki prihaja iz podjetja, ki trži skenerje in seveda zagovarja skeniranje kot varnostni ukrep in g. Bussbachom, kot predstavnikom letališča, ki je tudi bolj na strani nujnosti novih ukrepov po letališčih. Med seboj se gospodje pogovarjajo v nemščini in angleščini, del filmskega zapisa se zaradi hrupa iz okolice slabše sliši, zato sem napisal povzetek dogajanja. Pri tem sem sledil bolj smislu in pomenu filma oziroma oddaje, ki je kljub časovni distanci še vedno aktualen.

Vse dogajanje v prvem kadru je v zaprtem studiu, kjer je pripravljen tudi telesni skener. Voditelj predstavi izhodišče o temi z besedami: »Praktično to torej pomeni, da s skenerjem ni mogoče ničesar zaznati, kar je skrito v telesu. Kako varno je sploh to?«

Prof. Gruber pojasnjuje: »To kar vidite tu je pasivni telesni skener, ki deluje v območju med infra rdečim in mikrovalovnim valovanjem. Zaznava telesno in druge oblike toplote kot infra rdeče valovanje, čeprav naše telo oddaja tudi druga valovanja, ki se lahko križajo z valovanji okoliških teles ali naprav. V primeru, da ima oseba pri sebi nek predmet, bi ta na mestu, kjer se nahaja blokiral valovanje, ki ga povzroči telo in to bi skener zaznal v obliki belih lis kot predmet ob telesu (ostala nemoteča valovanja prikazuje v obliki rdečih lis opomba E.Š.).

Voditelj predlaga Gruberju: »Prav predlagam, da preizkusimo ta skener in poglejmo, če bo zaznal vse predmete, ki jih Vi nosite ob telesu.«

Prof. Gruber je odšel do skenerja, tam dvignil roki in počakal, da ga je naprava preskenirala. Po samem postopku je povedal, da je imel pri sebi poleg mobilnega telefona, ki ga je skener zaznal tudi švicarski nož, ki se na zaslonu skenirane slike telesa ni dovolj jasno videl. G. Haskett je pojasnil, da žepnega noža ni bilo videti, ker bi se ob pravem skenerju na letališču moral prof. Gruber ali drug potnik obrniti za sliko z bočne strani. Tako bi se nož jasno videl s strani. Gruberju so tako odvzeli mobilni telefon, videti je bilo tudi mikrofon, ki so ga pustili.

Novinar je po tem pregledu prof. Gruberja vprašal, če je imel še kaj pri sebi?

Gruber je odgovoril: »Da, še precej stvari.« Iz ust je potegnil belo ampulo in povedal, »To je vžigalnik«, iz žepov je potegnil nekaj manjših plastenk. Tu je snov Termit, ki gori s 4000°C.

Voditelj je povprašal: »In vse to ste imeli v žepih v času, ko ste se skenirali?«

Gruber je temu pritrdil in medtem naslonil nogo na dvignjen podstavek rekoč: »Za tem lepilnim trakom imamo epruveto, ki bi jo uporabil za mešanje ustreznih razmerij eksploziva, da bi povzročil nastanek najmanj velike luknje v letalu če ne celo kaj več.

G. Haskett je predlagal: »Poglejmo si še enkrat sliko skeniranja.«

Voditelj se je strinjal z besedami: »Kako je to, kar vidimo, sploh mogoče?« Prof. Gruber je iz žepa potegnil še plastični vžigalnik, ki ga uporabljajo kadilci za prižiganje cigaret in rekel: »Tukaj v žepu suknjiča imam še vžigalnik.« Torej je imel g. Gruber dva vžigalnika. Eden je bil za vžig eksplozivnega telesa in drugi za vžig tega vžigalnika z ognjem. G. Haskett je malo v zadregi vskočil v besedo: »Naj vam pojasnim. Tukaj nismo na letališču. Tam bi moral prof. Gruber suknjič odložiti. Povedal sem vam že, da bi pri predpisanem pregledu posneli sliko tudi s strani. Poglejte njegov suknjič, ki sploh ni ob telesu, zato magnetno valovanje ni bilo ustavljeno. Žal pa v resnici ne vidimo stvari v ustih ali drugih predelih telesa, ki so pod površjem. Noben sistem ni popoln. Vedno se najde kakšna pomanjkljivost. Prikriti bi bilo možno tud stvari pod kožne gube pri debelejših ljudeh. Tudi v primeru, če bi oseba kak predmet pogoltnila ali če bi postavila tak predmet pod stopala je ne bi videli. Kljub temi nudi skeniranje zelo dobro osebno preiskavo brez tipanja druge osebe.«[6]

Bussbach ugotavlja, da skeniranje vendarle ne zagotavlja visoke varnosti in zato nima smisla uporabljati še eno napravo, ki bo prispevala le delček k celoti. Vprašanje, ki se pojavi je ali lahko s tako segmentiranimi varnostnimi ukrepi dosežemo ustrezno varnostno prednost.

Druga scena oddaje je na odprtem prostoru v zimskem okolju večera. Voditelj predlaga, da bi odšli na dvorišče, kjer bodo preverili pravilnost napovedi g. Gruberja o učinkovitosti Termita in posledicah, ki jih lahko povzroči. Vsi se oblečejo v zimska oblačila razen g. Gruberja

Prof. Gruber je še pojasnil: »Namenoma nismo prej napravili eksploziva. Preprosto imam Termit, ki ga je lahko izdelati. Je gorljiv in pri gorenju povzroča več kot 4000°C toplote. Manj natančna razmerja pri mešanju tak dosežek znižajo, vendar lahko brez posebno natančnega merjenja napravim zmes, ki bo povzročila 3000°C vročine. Takšnega požara ni mogoče enostavno pogasiti z gasilniki.«

Voditelj še vpraša Gruberja: Kje ste dobili ta Termit?«

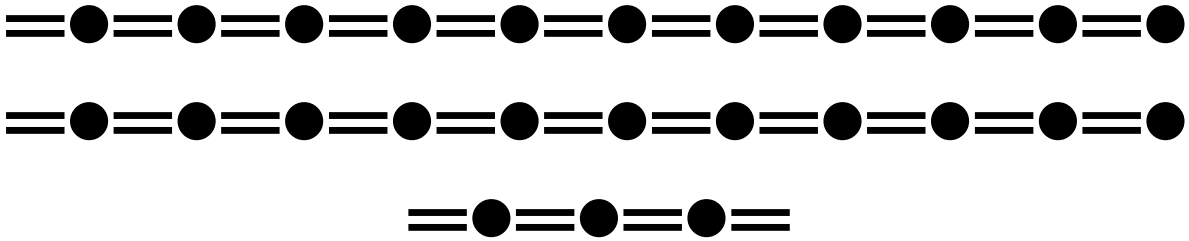
Gruber odgovori, da se vse lahko dobi v drogeriji.

Voditelj začudeno: »Torej ga je moč kupiti v drogeriji ali bolje založeni trgovini z gradbenim blagom? Kaj se bo zdaj zgodilo?«

Gruber še doda: »To vse kar vidite je v vrednosti nekaj centov. Človek, ki pozna potrebna razmerja, o čemer ne bi želel tu v javnosti govoriti, lahko dosežete temperature, ki talijo kovine.« Najavi tudi, »Sedaj bomo prižgali vse skupaj. Predlagam, da se malo umaknete.«

G. Bussbach medtem povzame: »Zato so kontrole na letališču. Preprečiti je potrebno, da se škodljive snovi vzamejo na letalo. Prav iz tega razloga se ukvarjamo z raziskovanjem varnosti s pomočjo podjetij, civilne družbe in institutov.«

G. Gruber med delom doda: »Če bi dodali še vodo, bi se vse skupaj razlilo. Verjetno bi prišlo do eksplozije. V posodi kamor smo dali Termit se je napravila luknja. V letalu bi to teroristi naredili nad vodniki in jih povsem uničili. Pri Boeingu 747 je to v levem sprednjem delu.«



6. *Prof. Gruber je močnejše postave in morda sta ga nasprotnika skušala »iztiriti« z opominjanjem, da je njemu zaradi maščobe lažje skriti predmete pred skeniranjem. Vprašanje je ali bodo bodoči teroristi debelejši ljudje? Ali bodo debelejše potnice in potnike skrbnejše pregledovali?*

   Med samim prikazom je bil dr. Gruber oblečen v ohlapno obleko. Suknjič je imel ves čas odpet, tako da je bilo še več prostora med njegovim telesom in samo obleko.

G. Bussbach precej jezno zaradi nasprotnega mnenja ostalih doda: »Zdi se mi, da je to samo delno lahko smešno, saj je sporočilo tega vašega primera, kako naj ravnajo teroristi po metodi nekega profesorja.«

Voditelj je spravljivo vskoči v besedo: »Sploh ne gre zato. Želimo le povedati, da je prav za prav strašljivo, da nam na letališču vzamete steklenico vode, medtem ko je mogoče tako enostavno priti mimo kontrol in prenesti tako nevarno snov na letalo.«

G. Bussbach zagotovi: »Zato moramo skrbeti, da takšne snovi ne pridejo na letalo. Prof. Gruber je po moje predvsem želel pokazati, da obstojajo nevarne snovi, ki jih detektorji kovin sploh ne zaznajo. Kar se tiče vnašanje tekočin je to predpisano z uredbo EU in kot vsak predpis ima tudi pomanjkljivosti.« (opis prenosa tekočin je naveden v tekstu pred tem).

Voditelj zaključi: »Gre predvsem za to, da ugotovimo zakaj je potrebno vodo oddati, medtem ko na letalo lahko vzamemo snovi, kot je pokazal profesor Gruber in tega nihče kljub

skeniranju ne opazi.«

Voditelj nadaljuje: »Večina nasprotnikov uvajanja skenerjev je mnenja, da so skenerji le navidezno najboljša rešitev za povečanje varnosti na letališčih. Prepričanje o vplivu teh naprav na varnost lahko doseže povsem nasprotni učinek, ko se bomo zanašali na napravo se bo s njeno uvedbo nivo varnosti celo znižal.«

Toliko o tej oddaji. Dodam le še to, da je Termit v bistvu železov oksid, bolj znan kot rja in aluminij. Če se zmeša drobno zdrobljen aluminij v razmerju, ki je še enkrat večji od deleža zdrobljenega železovega oksida dobimo to snov. Stvar seveda le ni tako enostavna, kar lahko vidimo tudi na spletni strani http://en.wikipedia.org/wiki/Thermite, kjer za to snov navajajo tudi, da je to $Fe2O3 + 2Al \rightarrow 2Fe + Al2O3$ ali $3CuO + 2Al \rightarrow 3Cu + Al2O3$. Naslednji problem je vžigalnik, ki to snov lahko zaneti. Podobno kot pri dinamitu ali atomski bombi, kjer je največ dela z visoko oplemenitenim plutonijem ali uranom. Moramo imeti ustrezno snov, ki povzroča pravo vrsto iskrenja, ognja ali eksplozije, ki prižge eksplozivno snov.

Ta eksplozivna snov je bila znana že v drugi svetovni vojni. Obstoja več podzvrsti. Med njimi je najbolj znan nanotermit, ki se dobi še s preciznejšim drobljenjem substanc in mešanjem. V teorijah zarote (ki se večkrat pojavlja v tem tekstu) navajajo, da so ta eksploziv uporabili pri rušenju stavb WTC ob navideznem napadu teroristov z letali.

Snovi, ki povzročajo eksplozije, gorenje, taljenje kovine in podobno je v naravnem okolju še precej. Že sam smodnik, ki ga je po eni od pripovedi naredil menih Schwartz kot alkimist, in mu je pri tem razneslo laboratorij, stari Kitajci pa so ga menda poznali že tisoč let pred našim štetjem, je sestavljen iz kalijevega nitrata (umetno gnojilo ali čilski soliter), žvepla in oglja. Kalij je v kombinaciji z natrijem eksploziven ob dodajanju vodika.

Tu je še vrsta radioaktivnih snovi in drugih snovi, ki eksplozivno reagirajo na dodajanje vode in (samo)segrevanje, kot so celzij in rubidij in še bi lahko naštevali, vendar bi ta moj tekst lahko kdo razumel kot priročnik za teroriste. Želim le poudariti, da varovanje pred eksplozijami ni enostavno in opominjam na možnosti, da so lahko preteča nevarnost realizira tudi v naših poslovnih okoljih. Pri tem se je potrebno spomniti kako enostavno se pride do nevarnih snovi tudi na trgu zaradi bližine vojaških bojišč in slabo varovanih vojaških skladišč.

4. ZAKLJUČEK

EU se je z Lizbonsko pogodbo obvezala, da bo spoštovala vse človekove pravice. Tu nam prav pride pravno orodje načelo sorazmernosti, ki ga uporablja tudi Evropsko sodišče za človekove pravice v Strasbourgu in čedalje pogostejše tudi nacionalna sodišča, ko tehtajo med različnimi pravicami posameznikov in skupnosti. Evropsko sodišče za človekove pravice k spoštovanju zasebnosti zavezuje tudi 3. člen Evropske konvencije o človekovih pravicah, ki pravi, da se s človekom ne sme ravnati ponižujoče [Šinkovec 1997, 53].

Pravnih virov in podlag je o tej temi mnogo več. To je tudi 17. člen Ustave RS, ki implicitno obravnava tematiko v pravici do življenja in telesno nedotakljivost in tudi temelji prava kot so šola naravnega prava in vedenje o družbeni pogodbi [Šikovec 1997, 48].

Ustava pa eksplicitno o tej človekovi pravici piše v 34. členu, kjer navaja, da ima vsakdo pravico do osebnega dostojanstva in varnosti [Šikovec 1997, 43].

Za uvedbo skenerjev na letališčih se je februarja letos odločila avstralska vlada. Premier Kevin Rudd si je zelo prizadeval za uvedbo teh naprav ne glede na očitke nasprotnikov, da se bo čas pregledovanja povečal in zato bodo večje zamude letal. Morda ni to nič nenavadnega, če ob tem upoštevamo povezanost Avstralije z Ameriko. Žal pa so mediji v aprilu letos poročali tudi o tridnevnem pridržanju turistke, ki je v Avstralijo pripotovala na prijetno druženje, a so jo na letališču osumili prenosa nedovoljenih snovi, čeprav je v svoji steklenici imela le osvežilno pijačo znanega proizvajalca, ki si jo je za na pot kupila v domači trgovini. Turistka je za medije povedal, da so avstralski varnostniki delali z njo precej grobo.

Skenerje so uvedli tudi v Italiji. Njihov minister še vedno zagovarja stališče, da je to ustrezna tehnologija, ki jo je potrebno uporabiti, ko je na razpolago. Kaj Italijane in ostale Evropejce še čaka? V letošnjem letu naj bi odpravili omejitve pri vnosu tekočin. V ta namen se preizkušajo posebni skenerji, ki bodo kontrolirali tekočine, ki jo ima potnik za svoje potrebe v svoji osebni prtljagi. Torej bo to še en skener v paleti drugih, ki naj bi prepoznaval nevarne snovi in jih ločeval od drugih tekočin. Ali bomo vse pomisleke o njegovi uvedbi premleli še enkrat?

Seveda pa ob vsem tem ne miruje propaganda teroristov. Napovedali so in v praksi smo tudi že videli nekaj poizkusov posodobljenega načina prenosa eksplozivnih substanc mimo letaliških kontrol, ki bodo opremljene s telesnimi skenerji.

Po objavi britanske civilne obveščevalne službe MI5 naj bi Al Kaida svojim pristašem, ki se odločijo, da bodo postali samomorilski napadalci v njihova telesa s kirurškim posegom vstavili eksplozivne snovi. Omenja se eksploziv Pentrit ali PETN, ki dosega eksplozivno hitrost (hitrost širjenja eksplozije) do 8300 metrov v eni sekundi in ne zahteva posebnih vžigalnikov. Po istemu viru naj bi vžigalnik bila kar injekcijska brizgalka z iglo v kateri naj bi bil aceton peroksid. Eksplozijo pa bi lahko povzročil tudi padec na trdo podlago z večje višine. Injekcijske igle ali podoben sistem za vnašanje eksplozivnega sredstva v telo, bi lahko bili tudi »peresniki«, kot navidezni pripomočki za vnašanje inzulina pri sladkornih bolnikih.

To je vrsta podlag za različna teroristična dejanja tudi v prihodnjih mesecih in letih. Incident pa niso samo dejanja teroristov pač pa vsako dejanje, ki ni formalizirano in predpisano po definiciji ISACA. Na ta dejanja, v opisanih oblikah, pa je potrebno opozoriti tudi v naših poslovnih okoljih in jih predvideti v varnostnih politikah in varnostnih načrtih. Varnost je sama po sebi zelo širok pojem.

Literatura:

Gordon Thomas, skrivnostna zgodba Mosada, Učila Inernational, Tržič 2002

Southwell David in Twiat Sean, Dosjeji zarot (Drzno potovanje do skrajnih meja preganjavice, skrivnosti in spletk po sveti (v originalu Conspiracy files, Carlton Books Limited iz leta 1999) Mladinska knjiga založba d.d., Ljubljana 2004

Šinkovec Janez, Pravice in svoboščine, Časopisni zavod Uradni list Republike slovenije, Ljubljana 1997

Reference:

Skico sem prenesel iz prezentacije, ki sem jo oblikoval za temo Meje moje zasebnost. Predavanje o tem je bilo v sklopu foruma Varna tajnica 13.11.2008 v Novi Gorici.

Viri:
Konferenca v Toledu je bila predstavljena v radijski oddaji Studio ob 17 v ponedeljek 25.01.2010 z naslovom oddaje Skenerji na letališčih-nujni za varnost
Učinkovine Termit tudi na: http://www.youtube.com/watch?v=Yex063_Fblk

Vdor v zasebnost na letališču iz opombe 4, je na spletni strani http://www.zurnal24.si/svet/skener-letalisce-gol-nadlegovanje-164796, kjer so tudi različni komentarji naključnih bralcev.

Zgodovinski podatki o teroristih in ugrabitvah letal so iz Wikipedije