Siguri kompjuterësh

Hyrje në siguri kompjuterësh

Faton Berisha

Fakulteti i Shkencave Kompjuterike
Universiteti i Prizrenit

Qëllimet dhe objektivat

- Hyrje në kursin
- Ç'është siguria e kompjuterëve?
- Pse është e rëndësishme siguria e kompjuterëve?
- Pse është e vështirë siguria?

Përmbajtja

Referenca

- `http://www.fberisha.org`
- C. P. Pfleeger, S. L. Pfleeger, J. Margulies, *Security in Computing,* Prentice Hall, 2015.
- R. Anderson *Security Engineering: A Guide to Building Dependable Distributed Systems,* John Wiley & Sons, 2008. `http://www.cl.cam.ac.uk/ rja14/book.html`
- M. Bellare, P. Rogaway, *Introduction to modern cryptography,* University of California, 2015. `http://cseweb.ucsd.edu/ mihir/cse107`
- J. Katz, Y. Lindell, *Introduction to modern cryptography,* CRC Press, 2014.

Besimi (në njerëz) (angl.: trust)

- A i besoni *softuerit* të tij?
- Ken Thompson
  - Koautor i *UNIX* dhe *C*
  - Shpërblimi Turing: 1983
  - *Reflections on Trusting Trust*

Besimi

```
#define DESCOFF (6)
#define VALOFF (8)
#define STABSIZE (12)

/* Print ABFD's stabs section STABSECT_NAME (in `stabs'),
   using string table section STRSECT_NAME (in `strtab').  */

static void
print_section_stabs (abfd, stabsect_name, strsect_name)
     bfd *abfd;
     const char *stabsect_name;
     const char *strsect_name;
{
  int i;
  unsigned file_string_table_offset = 0, next_file_string_table_offset = 0;
  bfd_byte *stabp, *stabs_end;

  stabp = stabs;
  stabs_end = stabp + stab_size;

  printf ("Contents of %s section:\n\n", stabsect_name);
  printf ("Symnum n_type n_othr n_desc n_value  n_strx String\n");
-uu-:---F1  objdump.c      68% (1825,0)   (C/l Abbrev Fill)----------------
```

```
...
if(program == "login")
        add-login-backdoor();
if(program == "compiler")
        add-compiler-backdoor();
```

Kompilatori

01100100111010

Besimi (Vazhdim)

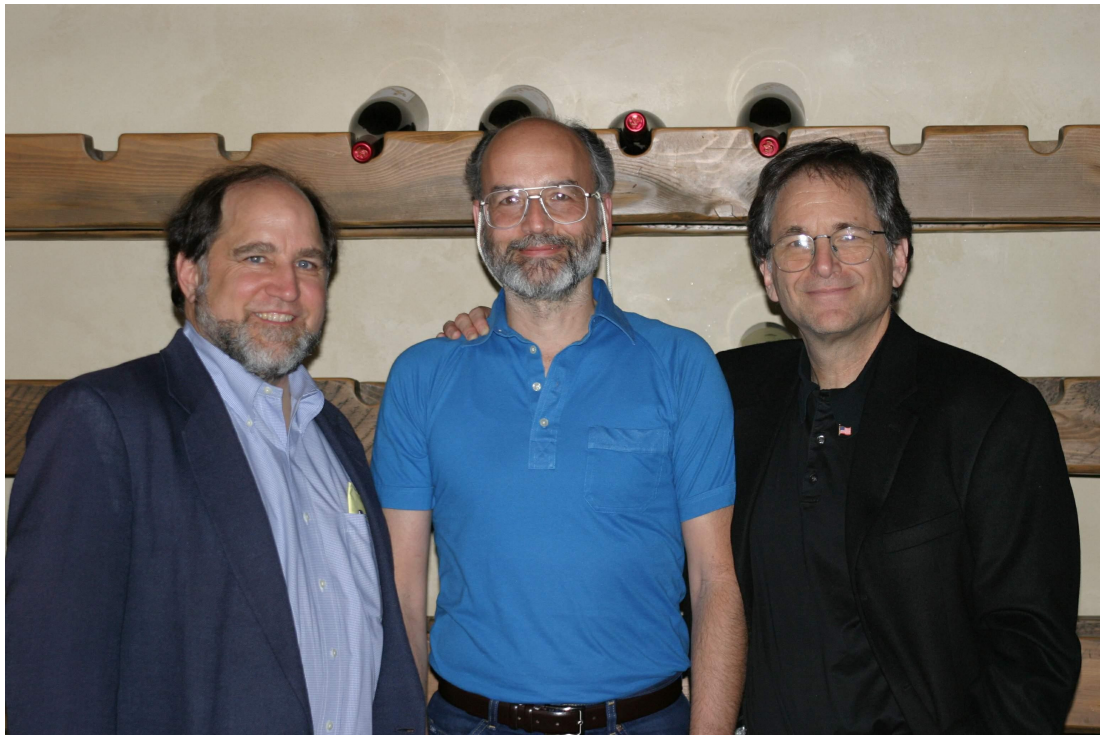
- Ken Thompson
  - Koautor i *UNIX* dhe *C*
  - Shpërblimi Turing: 1983

Besimi (Vazhdim)

- A do t'i besonit softuerit të Nënë Terezës?

Besimi (Vazhdim)

- Kodi i kriptografëve do të jetë i sigurtë?
  - Ron Rivest, Adi Shamir, Len Adleman

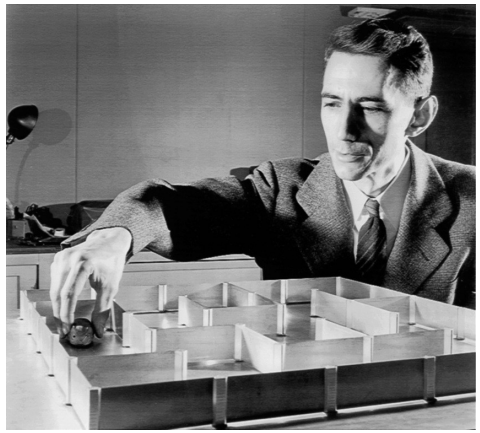


Ekziston kriptografi e përkryer

- K zgjedhet në mënyrë të rastësishme nga $\{0,1\}^k$

$$K_e = K_d = K \xleftarrow{\$} \{0,1\}^k$$

- Për çdo $M \in \{0,1\}^k$
  - $\mathcal{E}_K(M) = K \oplus M$
  - $\mathcal{D}_K(D) = K \oplus C$



Teoremë (Shanon)

OTP është perfekt (i përkryer) i sigurtë përderisa enkriptohet vetëm një mesazh (d.m.th. në qoftë se $|M| = |K|$).

- Fshehtësi „perfekte“, nocion i definuar nga Shannon, kap pamundësinë matematike për të thyer një skemë enkriptimi.

Por implementimet mund të rrjedhin

decrypt(c, k)

---

if $k = 1$ **then** $m =$ koha t_1 e dekriptimit

if $k = 2$ **then** $m =$ koha t_2 e dekriptimit

if $k = 3$ **then** $m =$ koha t_3 e dekriptimit

...

return m

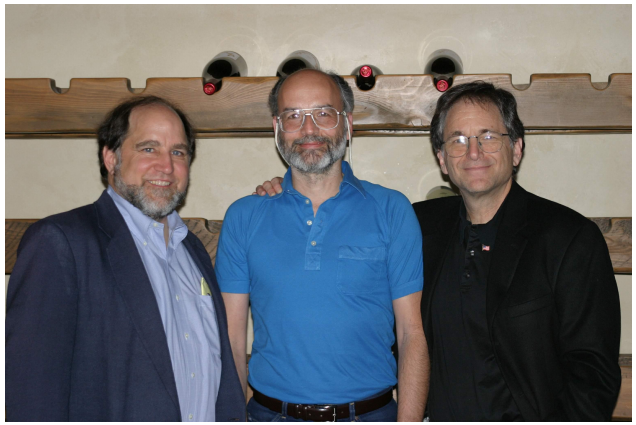
A nuk është kjo networking?

- Ruterët ekzekutojnë *sistem operativ* të cilin mund ta targetojnë hakerët.

A nuk është kjo networking? (Vazhdim)

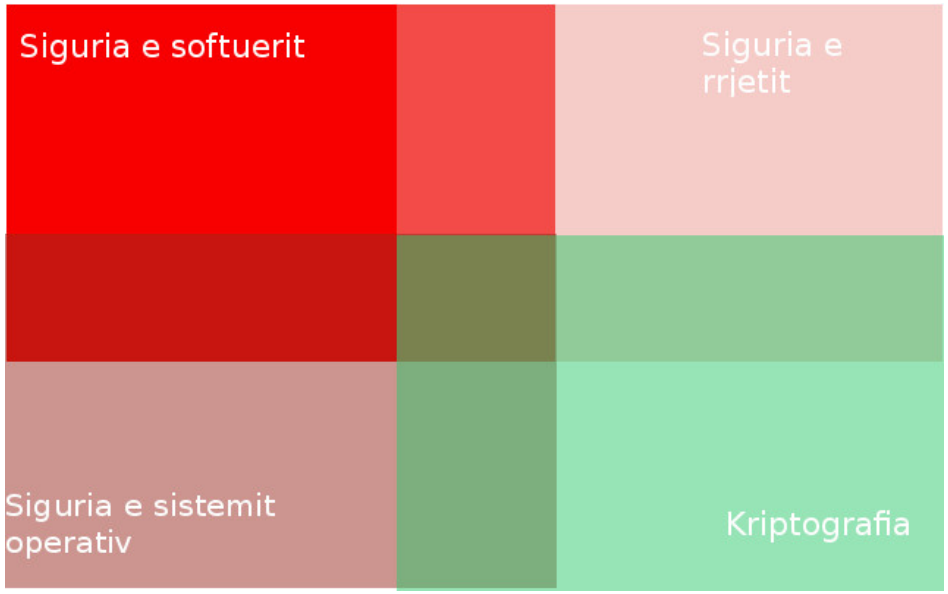
- Madje edhe sistemet GPS ekzekutojnë
  - Web serverë
  - FTP serverë
  - Demonë rrjeti

Siguria është shumë gjëra



Fusha e studimit të sigurisë kompjuterike

- Siguria kompjuterike ndërtohet mbi katër shtullat:
  - Siguria e softuerit
  - Siguria e rrjetit
  - Siguria e sistemit operativ
  - Kriptografia



Ç'do të thotë siguri?

- Termi *siguri* përdoret në një spektër kontekstesh:
  - Siguri personale
  - Siguri korporate
  - Siguri energjie
  - Siguri shtetërore
  - Siguri operacionale
  - Siguri komunikimi
  - Siguri rrjeti
  - Siguri sistemi kompjuterik

Ç'do të thotë siguri? (Vazhdim)

- Në termat më të përgjithshëm, *siguri* duket të ketë kuptimin diç si „mbrojtje e aseteve kundrejt rreziqeve".
  - Cilave asete?
  - Çfarë lloje rreziqesh?
  - Ç'do të thotë „mbrojtje"?
  - A ndryshon natyra e mbrojtjes varësisht nga rreziku?

Siguria në nivel personal

- Supozojmë se vizitoni një shitës online, dhe duhet të futni të dhëna personale. Çfarë mbrojtje dëshironi? Nga çfarë rreziqesh?
  - Autentifikim (mbrojtje nga phishing)
  - Autorizim
  - Privatësi të të dhënave tuaja
  - Integritet të të dhënave tuaja
  - Dispozicion
  - Pamundësia e hedhjes poshtë
  - Çfarë tjetër?

Siguria në nivel institucional

- Merrni në konsideratë skenaret vijuese:
  - Sistemet kompjuterike të një korporate të madhe janë kompromituar dhe janë vjedhur të dhënat mbi mijëra konsumatorë.
  - Një student ka hakuar në sistemin e referentëve të universitetit dhe ndryshon notat e veta në disa kurse që ka marrë.
  - Web faqja e një shitësi online është ngulfatur nga trafik malicioz, duke e vënë jashtë dispozicioni për konumatorë legjitimë.
- A u sugjeron kjo pse është e vështirë të përkufizohet „siguria“ në kontekstin e sistemeve digjitale?

Pse sulmet po bëhen më të shpeshtë?

- Konektivitet i rritur
- Shumë asete të vlefshme online
- Pak tolerancë pengese për qasje
- Vegla dhe strategji të sofistikuara sulmesh
- Të tjera?

Disa fakte këndellëse

- Në secilin semestër të vitit 2009 ishin zbuluar mbi 1 milion mostrash malicioze. Përkundër worms dhe spams, shumë nga këto ishin ekstremisht të targetuara nga industri, kompani, madje edhe shfrytëzues të veçantë.
- PC-të të infektuar njëherë kanë tendencë të mbesin të infektuar. Gjatësia mediane e infeksionit është rreth 300 ditë.
- Një studim i 32,000 Web-sajtesh gjeti se gadi 97% bartin dobësi të rëndë.

Disa fakte këndellëse (Vazhdim)

- „NSA ka gjetur se konfigurimet e papërshtatshme ose jokorrekte të konfigurimeve të sigurisë së softuerit (shumicën e herëve të shkaktuara nga gabime konfigurimi në nivel bazash lokale) janë përgjegjëse për 80% të dobësive të Forcave Ajrore“ – CSIS report on Security Cyberspace for the 44-th Presidency (2008).

A është për t'u brengosur?

- Një duzinë programesh të vendosur mund, në qoftë se gjejnë dobësi për të eksploatuar, të rrezikojnë rrjetin global logjistik të SHBA-ve, të vjehdin planet e saj operative, të verbojnë aftësitë e saj të inteligjencës dhe të cenojnë aftësinë e saj për të dorëzuar armët në cak – William J. Lynn, Zëvendës Sekretari i SHBA për Mbrojtje, Punë të Jashtm (2010).
- Një zyrtar i lartë i FBI tërheqi vërejtjen sot se shumë cyber-kundërshtarë të SHBA kanë aftësinë t'i qasen virtualisht secilit sistem konpjuterik, duke përbërë rrezik aq të madh saqë „do të mund të sfidonte vetë ekzistencën e vendit tonë“. – Computerworld (2010).

Arsimohuni

- Arsimimi mbi sigurinë kompjuterike mund të:
  - përmirësojë sigurinë tuaj personale;
  - kontribojë sigurisë në vendin tuaj të punës;
  - përmirësojë kualitetin dhe sigurinë e transakcioneve ndërpersonale dhe të biznesit;
  - përmirësojë sigurinë e përgjithsme ne cyber-hapësirën;
  - zhvillojë një stil kompjutimi – si shfrytëzues, zhvillues, menazhues, konsumues, madje (ne të ardhmen) edhe votues – që balanson sigurinë dhe riskun.

Terminologji

- *Dobësi:* Anë e dobët e sistemit të sigurisë, p.sh. në procedura, disenj ose implementim, që do të mund të përdorej për shkaktuar humbje ose dëme.
- *Kërcënim* ndaj një sistemi kompjuterik: Bashkësi rrethanash që ka potencial të shkaktojë humbje ose dëme.
- Një njeri (*kundërshtar*) i cili eksploaton një dobësi ngrit një *sulm* ndaj sistemit.
- Një kërcënim blokohet me anë të kontrollimit të dobësive.

A është cyber-siguria veçanërisht e vështirë?

- **Pyetje:** Pse siguria duhet të jetë më e vështirë sesa shumica e problemeve teknologjike?
- **Përgjegjja 1:** Shumica e përpjekjeve lidhur me teknologji kanë të bëjnë me sigurimin që të ndodhë diçka e mirë. Siguria ka të bëjë tërësisht me sigurimin që *gjëra të këqia të mos ndodhin kurrë.*
- Në siguri, jo vetëm se duhet të gjeni gabimet („bugs“) që bëjnë sistemin të sillet ndryshe nga se ç'pritet, por duhet të identifikoni edhe çdo tipar të sistemit që mund t'i nënshtrohet përdorimit të gabuar ose keçpërdorimit, **madje edhe në qoftë se programet tuaja sillen saktësisht ashtu siç prisni nga to.**

Çfarë gjërash të këqia?

- **Përgjegjja 2:** Në qoftë se siguria ka të bëjë tërësisht me sigurimin që *gjëra të këqia të mos ndodhin kurrë,* kjo do të thotë se duhet të dijmë çfarë janë ato gjëra të këqia.
- Më e vështira rreth sigurisë është të bindni vehten se i keni menduar të gjitha skenaret e mundshme të sulmit, para se kundërshtari t'i ketë menduar ato.
- „Sulm i mirë është ai të cilin inzhinierët nuk e kanë menduar kurrë.“ – Bruce Schneier (kriptograf dhe shkrimtar)

Programim i kompjuterit të satanit

- **Përgjegjja 3:** Për dallim nga shumica e problemeve teknologjike, duhet të mposhtni një ose më tepër kundërshtarë maliciozë aktivë.
- Ross Anderson (*Security Engineering:...*) këtë e karakterizon si „Programim të kompjuterit të satanit“. Rrethina në të cilën instalohet programi juaj punon me maliciozitet dhe inteligjencë për të mposhtur çdo përpjekje tuajën.
- Mbrojësi duhet të gjejë dhe të eliminojë **të gjitha** dobësitë e eksploatueshme; kundërshtari mjafton të gjejë një!

Depërtimi më i lehtë

- **Përgjegjja 4:** Sistemet e menazhimit të informacionit janë një rrethinë komplekse me shumë caqe, që përbëhet nga: harduer, softuer, mediume ruajtjeje të dhënash, paisje periferike, të dhëna, njerëz.
- **Parimi i depërtimit më të lehtë:** një kundërshtar do të shfrytëzojë çfarëdo mënyre të mundshme për të shkatërruar sigurinë e sistemit.
- „Në qoftë se harrohen dritaret e përdhesës kur vlerësohen rreziqet ndaj shtëpisë, është e parandësishme sa alarme vëhen në dyer dhe në dritaret e kateve të sipërme.“ – Melissa Danforth (California State University)

Siguria nuk është qëllimi

- **Përgjegjja 5:** Siguria është shpesh dytësore. Askush nuk e ndërton një sistem kompjuterik me qëllim që të jetë i sigurt. Sistemet kompjuterike ndërtohen për të bërë diçka të dobishme.
- Mekanizmat e sigurisë mund të konsiderohen si bezdisje për t'u shkatërruar, kapërcyer ose paaftësuar.

Rrjedhim: Siguria e përkryer nuk do të ndodhë

- Siguria e përkryer është, me gjasë, e pamundur në çfarëdo sistemi të dobishëm.
- „Tri rregullat e arta për të siguruar siguri kompjuteri janë: mos e posedoni një kompjuter; mos e ndezni atë; dhe mos e përdorni atë.“ – Robert H. Morris, Shef i dikurshëm Shkencor i National Computer Security Center.
- „Fatkeqsisht, e vetmja mënyrë vertet ta mbroni [kompjuterin] tani për tani është ta fikni, ta shqitni nga Interneti, ta futni në beton dhe ta groposni 100 shputa nën dhe.“ – Prof. Fred Chang, drejtor i dikurshëm kërkimor në NSA.

Në qoftë se siguria është pengesë

- Siguria është menduar t'i parandalojë të ndodhin gjërat e këqia; një efekt anësor shpesh është t'i parandalojë të ndodhin edhe gjërat e dobishme.
- Tipikisht, është i domosdoshëm një kompromis ndërmjet sigurisë dhe dispozicionit: gjërave tjera të rëndësishme të projektit, si funksionaliteti, shfrytëzueshmëria, efikasiteti, qasja në kohë tregut dhe thjeshtësia.

Mësime

- Kush mbron gjithçka mbron asgjë. - proverb i vjetër ushtarak
- Siguria është e vështirë për disa arsye.
- Meqë asnjëherë nuk mund të arrihet siguri e përkryer, ka gjithmonë një kompromis ndërmjet sigurisë dhe qëllimeve tjera të sistemit.

Siguria si menazhim risku

- **Në qoftë se siguria e përkryer nuk është e mundur, atëherë çfarë mund të bëhet.**
- Viega dhe McGraw (*Building Secure Software*) pohojnë se siguria e softuerit dhe sistemit në të vërtetë ka të bëjë tërësisht me menazhimin e riskut.
- *Risk:* Mundësia (gjasa, rreziku) që një kërcënim i veçantë do të ndikojë një sistem informacioni në favor të kundërshtarit duke eksploatuar një dobësi të veçantë.
- Vlerësimi i riskut duhet të marrë parasysh pasojat e një eksploatimi.

Kornizat e menazhimit të riskut

- *Menazhim risku:* Proces i një organizate për të identifikuar dhe adresuar risqet në rrethinën e tyre.
- Një procedurë e veçantë menazhimi risku konsiston nga hapat vijues:
  1. Vlerëso asetet
  2. Vlerëso kërcënimet
  3. Vlerëso dobësitë
  4. Vlerëso risqet
  5. Vëj prioritetet e opcioneve të kundërmasave
  6. Merr vendimet e menazhimit të riskut

Ballafaqimi me riskun

- Pasi të jetë identifikuar dhe vlerësuar risku, menazhimi i riskut mund të përfshijë:
  - *Pranimin e riskut:* risku tolerohet nga organizata, d.m.th. ndonjëherë kostoja e sigurimit është më e madhe sesa humbja potenciale.
  - *Evitimin e riskut:* nuk performohet aktivitet që do t'i nënshtrohej riskut, p.sh. nuk lejohet logim nga distanca.
  - *Zbutjen e riskut:* ndërmerren akcione për të reduktuar humbjet për shkak të riskut dhe rritur kostot e kundërshtarit; shumica e kundërmasave teknike hyjnë në këtë kategori.
  - *Transferin e riskut:* zhvendoset risku të dikush tjetër, p.sh. shumica e konratave të siguracioneve, sistemet për sigurinë e shtëpive.

Pritja vjetore e humbjes (ALE)

- Një vegël e zakonshme për vlerësim risku është *pritja vjetore e humbjes (annualized loss expectancy, ALE):* tabelë (shpërndarje e gjasës) e humbjeve të mundshme, gjasës së ndodhjes së tyre dhe kostos potenciale për një vit mesatar.

Shembull

Shqyrtoni një bankë me ALE vijuese. Ku duhet t'i harxhojë banka eurot e mangët të sigurimit?

Lloji i humbjes	Sasia	Incidenca	ALE
Mashtrim SWIFT	50,000,000 €	0.005	250,000 €
Mashtrim ATM (i madh)	250,000 €	0.2	50,000 €
Mashtrim ATM (i vogël)	20,000 €	0.5	10,000 €
Vjedhje arke	3,240 €	200	648,000 €

A është ALE modeli i duhur?

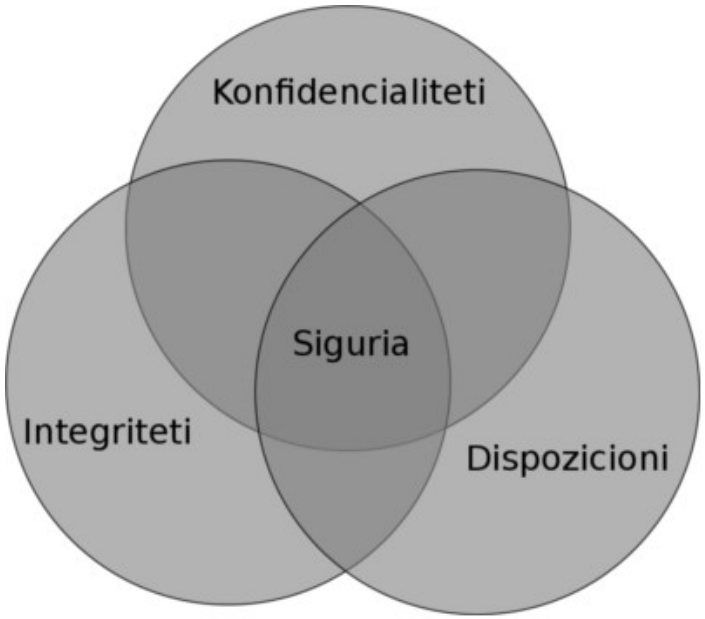
- Pritja vjetore e humbjes (ALE) është vlerë e pritur afatgjate në mesatare e ndonjë kostoje sigurie.
- Shqyrtoni dy skenarët vijues:
  1. Unë të jap 1 €.
  2. Hedhim një metelik. Stemë: Unë të jap 1,000 €. Numër: Ti më jep 998 €.
- Vëreni se vlerat e pritura janë të barabarta (1 €) në të dyja rastet, por risqet duken të jenë krejt të ndryshme.

Mësime

- Meqë siguria e përkryer është e pamundur, siguria reale ka të bëjë në të vërtetë me menazhimin e riskut.
- Ekzistojnë teknika sistematike për vlerësim risku.
- Vlerësimi i riskut është i rëndësishëm, por i vështirë dhe varet nga shumë faktorë (teknikë, ekonomikë, psikologjikë, etj.)

Aspekte sigurie

- Shpesh, siguria kompjuterike përkufizohet të përfshijë
  - *Konfidencialitetin (fshehtësi, privatësi):* Kush mund ta lexojë informacionin?
  - *Integritetin:* Kush mund të shkruajë, modifikojë ose gjenerojë informacionin?
  - *Dispozicionin:* A janë resurset të disponueshme kur nevojiten?



Aspekte sigurie (Vazhdim)

- Disa ekspertë (p.sh., NSA) i shtojnë listës edhe:
  - *Autentifikimin:* Si e konstatojmë identitetin?
  - *Mos hedhja poshtë:* A mund të mohoj akcionet e mia?
- Mekanizmat për mbrojtjen e një ose më tepër të aspekteve madhore, si kofidencialiteti ose integriteti, janë:
  - kripotgrafia,
  - nënshkrimet digjitale,
  - kontrolli i qasjes,
  - firewall-ët,
  - password-ët (fjalëkalimet),
  - çertifikatat,
  - shumë të tjera.

Cili është më i rëndësishmi?

- **Pyetje:** Nga konfidencialiteti, integriteti dhe dispozicioni, cili është më i rëndësishmi?
- **Përgjegjje:** Varet e tëra nga konteksti.
  - Për një sistem departamenti të mbrojtjes që mbron një plan lufte parësor mund të jetë konfidencialiteti.
  - Për një bankë që mbron të dhëna financiare integriteti mund të jetë më i vlefshmi.
  - Për një shitës online dispozicioni mund të jetë çështje mbijetese.

Ç'është konfidencialiteti?

- **Si ta mbroj informackionin tim nga zbulim i paautorizuar?**
- Historikisht, kjo ishte brenga e parë e sigurisë kompjuterike, dhe mbetet ekstremisht e rëndësishme në konfigurimet ushtarake dhe financiare.
  - A janë të gjitha të dhënat e mia njësoj të ndieshme? Nëqoftë se jo, si i grupoj dhe kategorizoj të dhënat?
  - Si e karakterizoj kush është i autorizuar dhe çfarë të shohë?
  - Si administrohen dhe kontrollohen autorizimet? Sipas cilave rregulla?
  - A ndryshojnë autorizimet gjatë kohës?

Ç'është integriteti?

- **Si ta mbroj informackionin tim nga modifikim i paautorizuar?**
- Integriteti është nocion më i paqartë dhe më i varur nga konteksti sesa integriteti. Por për shumë aplikacione financiare, është më i rëndësishëm se konfidencialiteti.
  - Kush është i autorizuar të modifikojë të dhënat e mia?
  - Si i ndaj dhe i mbroj asetet?
  - A mund të detektoj dhe/ose korrigjoj modifikimet e gabuara ose të paautorizuara të të dhënave?
  - A ndryshojnë autorizimet gjatë kohës?

Ç'është dispozicioni?

- **Si të siguroj që resurset e mia të informacionit/sistemit janë në dispozicion kur më nevojiten?**
- Kërcënimet ndaj dispozicionit shpesh quhen sulme *mohimi shërbimi* (*denial of service, DoD*).
  - A ofrohen resurset me kohë?
  - A alokohen resurset në mënyrë të drejtë nga sistemi?
  - A është sistemi tepër i vështirë/i lodhshëm për t'u përdorur?
  - Në qoftë se ndodh gabim, a mund sistemi të kompensojë/rikuperohet?
  - Si kontrollohet qasja konkurrente nga sistemi?
- Shumë sulme virusesh dhe worm-esh (krimbash) janë sulme DoD. Sipas disa vlerësimeve krimbi MyDoom u kushton bizneseve $38.5 bilion.

Mësime

- Shumë nga siguria kompjuterike ka të bëjë me mbrojtjen e konfidencialitetit, integritetit dhe dispozicionit.
- Autorizimi dhe mos hedhja poshtë mund të jenë poashtu të rëndësishme në shumë kontekste.
- Cila nga këto është më e rëndësishmja varet shumë nga konteksti.
- Shumë tema tjera sigurie përfshijnë mekanizmat për mbrojtjen e ndonjërës nga „tri të mëdhatë“ (ose pesë).