

TSIT01 Datasäkerhetsmetoder

Föreläsning 4: Programvarusäkerhet

Ingemar Ragnemalm

01001001 01000011 01000111

Detta har hänt

Föreläsning 1: Prevention-detection-reaction, CIA mm

Föreläsning 2: Att mäta säkerhet, projekten, prioriteringar

Föreläsning 3: Websäkerhet, attackmetoder, labbarna

01001001 01000011 01000111

Att mäta säkerhet = projekten

Analysera situationen

Bena ut med CIA

Hitta hot, svagheter

Uppskatta sannolikheter, skada

Finn åtgärder, prevention-detection-reaction, och uppskatta effekt

Finn numeriska värden

Prioritera

01001001 01000011 01000111

Webbsäkerhet = labbarna

Principerna med Internet och webben

HTTP, HTML, databaser

Databasangrepp, XSS, CSRF

Labbarna, 21 obligatoriska

01001001 01000011 01000111

LABBARNA ÖPPNAS!

Labbsystemet öppnas på fredag klockan 18!

Uppdaterat labbmateriel kommer under veckan.

01001001 01000011 01000111

Guilherme tar över från nästa föreläsning

Kryptering, lösenordslagring, behörighet...

Vi ses på sista föreläsningen!

01001001 01000011 01000111

Dagens föreläsning

Programvarusäkerhet

Attackmetoder, underliggande svagheter

01001001 01000011 01000111

Föreläsningsfrågor

1. Hur får du in malware i din dator?
2. Hur kan hemliga data avslöjas genom programvarufel?
3. Vad kan hända om du slarvar med signed/unsigned?
4. Vad är skillnaden mellan CIA och AAA?

01001001 01000011 01000111

Software security - programvarusäkerhet

01001001 01000011 01000111

Software security - programvarusäkerhet

Websäkerhet = saker som körs genom webbläsare.

- Säkerhetshål i websidor
- Manipulering av webbläsardata
- Skadliga scripts

Programvarusäkerhet = program som körs lokalt eller på en server.

- Lokala säkerhetshål i befintlig programvara
- Malware

Ofta kopplade - malware kan installeras från websidor.

01001001 01000011 01000111

Malware

Nån jävel smusslar in skadlig kod i din dator för att sabba för dig eller stjäla av dig!

01001001 01000011 01000111

Typer av malware (1)

- Adware: Annonser integrerade i programvara (pop-up-annonser eller omdirigering av webbläsaren)
- Spyware: Programvara som registrerar din aktivitet, inklusive:
- Keyloggers: Program som registrerar tangenttryckningar
- Spammer programs: Program som används för att skicka stora mängder oönskad E-post
- Trojan: Ett program som verkar användbart men **BILD BORTTAGEN** som har dolda potentiellt skadliga egenskaper som undviker säkerhetsmekanismer.

01001001 01000011 01000111

Typer av malware (2)

- Virus: Malware som, när det körs, kopierar sig självt till annan exekverbar kod
- Worm/mask: Ett program som körs oberoende och kan kopiera in sig självt på andra system på nätverket genom att utnyttja säkerhetshål eller stulna lösenord
- Zombie/bot: Program installerade på en infekterad maskin som aktiveras för att göra attacker på andra maskiner

01001001 01000011 01000111

DDoS, Distributed denial of service

Attack för att blockera en websida. Troligen hämnd eller aktivist, men kan också göras för att dölja en annan attack.

Görs genom att accessa den från många noder på en gång.

Förbereds genom att installera malware (zombies) i andras datorer.

IOT-attacken var en sådan.

01001001 01000011 01000111

Hur får man in malware?

- Exploits: Kod som utnyttjar en speciell svaghet
- Backdoor/trapdoor: Mekanismer som går förbi normala säkerhetskontroller
- Drive-by download: Kod på websidor som utnyttjar svagheter i webbläsaren för att angripa klienten när sidan öppnas och installera program.
- Installera efter att ha lyckats logga in i systemet.
- Falsk programvara
- Hårdvara med skadlig kod

01001001 01000011 01000111

Falsk programvara

Programvara kan vara något annat än det utger sig för att vara.

- Legitima program som ändrats till att installera malware
- Program som i sig utför skada
- Piratkopior, "kloner" som bryter mot upphovsrätt

01001001 01000011 01000111

Skydd mot falsk programvara

Programvarubutiker kan göra kontroller

Varningar om program som laddats ner från Internet

Program kan ha identifikationsstämplar, riktighetskoder som kräver att programmet är oförändrat

Kontroller tar tid och kan hindra legitim programvara - och kan ge false positives! (Apple)

Risk för konflikter mellan integritet och tillgänglighet!

Se upp med okända websidor,

01001001 01000011 01000111

Falska websidor med infekterade program

Se upp med okända websidor: Bluffsidor med infekterade eller falska program.

 Posted by u/CorpCarrot 1 year ago 

107

 **Scam Website Pretending to be OBS Studio - Virus Warning**

[Guide](#)

Hey everybody! First time posting here, I just installed OBS to use NDI to stream from my gaming PC to my streaming PC and it's working great.

However, through this process I found that someone is promoting one website, and perhaps two, on google search to be at the top of the search list - a website that isn't obsproject.com. This website offers up a duplicate to the OBSproject homepage with the various download links. Every other link and page on these duplicate sites are broken and do not work.

If you download from any of the available links, the installer contains a virus (caught by my webroot antivirus software).

01001001 01000011 01000111

Verktyg för malware-script kiddies

- Attack-kits: Uppsättningar av verktyg för att generera malware automatiskt
- Rootkit: Uppsättning verktyg som används efter att angriparen har kommit in i systemet och har root/admin-rättigheter

01001001 01000011 01000111

Angrepp via inloggning

Angriparen vill komma in som "användare"

Knäck lösenord

Sök igenom systemet

Installera program (malware) som kan hitta läckor

01001001 01000011 01000111

Hur tar sig angripare in?

BILD BORTTAGEN

Ändrar sig över tiden!

1) Hitta mål. Vem vill du angripa? Angriparen identifierar och karakteriserar mål från öppet tillgänglig information, teknisk och icke-teknisk.

2) Första access: Hur kommer den in? Utnyttjar ofta säkerhetsläckor on-line, som svag autentisering eller malware via drive-by-download-attacker.

3) Utökning av privilegier. Väl inne, kan angriparen få administratörsprivilegier?

01001001 01000011 01000111

Hur tar sig angripare in?

- 4) Samla information eller utforska systemet. Kan göras för att navigera till annat mål.
- 5) Behålla access. Installera bakdörrar eller annan malware, eller genom att lägga till extra administratörskonton.
- 6) Dölja spåren. Ta bort eller ändra loggfiler som visar vad som hänt.

Säkerhetshål

Hur kan program ha säkerhetshål?

01001001 01000011 01000111

Säkerhetshål

Dålig säkerhet kan läcka information som låter angriparen komma vidare.

Detta kan innebära köra egna program som fiskar information.

Det kan också innebära att köra existerande program som under vissa förutsättningar kan läcka information.

01001001 01000011 01000111

Abstraktion: nödvändighet och risk

Abstraktion eller transparens?

01001001 01000011 01000111

Risker vid förändring och abstraktion

Förändringar skapar problem!

Även om du förstår vad ändringen går ut på så är det lätt att det blir fel.

Abstraktion är användbart för att förstå komplexa system... men kan dölja vad som verkligen händer.

Säkerhetsproblem är ofta så detaljberoende att det är ett problem att dölja detaljer.

Abstraktion vs transparens

01001001 01000011 01000111

Abstraktionsrisker: Heltal

Enkelt exempel: 8-bitars heltal, en byte:

8-bitars heltal "unsigned": 0 till 255

8-bitars heltal "signed": -128 till 127

Unsigned: $255 + 1 = 0$

Signed: $127 + 1 = -128$

255 unsigned = -1 signed

Demos:
signed-error-2
Integer overflow

01001001 01000011 01000111

Abstraktionsrisker: Heltal

Viktig insikt: Datorns heltal är inte samma sak som matematiskt heltal

$$b \geq 0 \not\Rightarrow a + b \geq a$$

Använd huvudsakligen "unsigned"

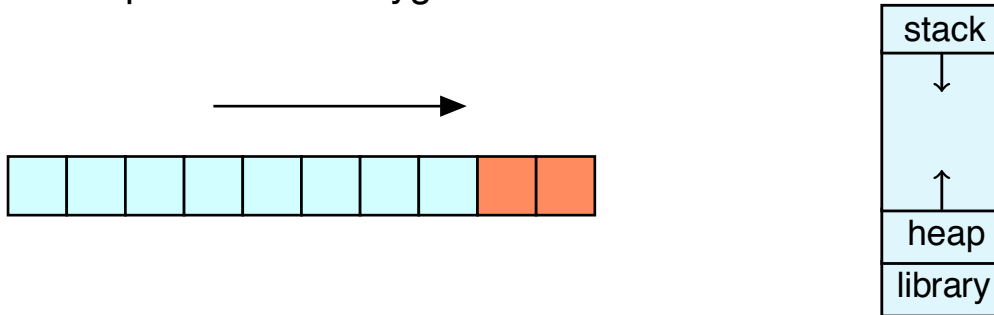
Se upp för overflow

Slå på varningar för operationer mellan signed och unsigned

01001001 01000011 01000111

Minneshantering

Accesser över buffergränser, buffer overruns. Stack overrun och heap overrun. Arraygränser.



01001001 01000011 01000111

Stack overrun

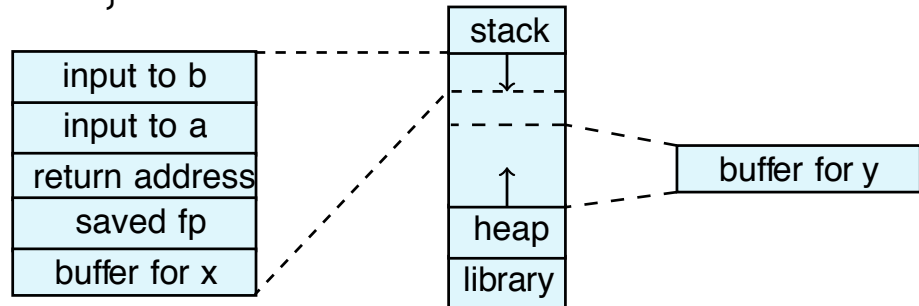
Vad händer när stack och heap tar slut?

Exempel:

```
void myfunction(int a, int b)
{
    char x[20];
    char *y = malloc(1000);
}
```

Läggs på stack

Läggs på heap



01001001 01000011 01000111

Stack overrun

Genom buffern som nu krockar med stacken kan ett program accessa data utanför de egna variablerna. Detta begränsas av minnessaccessrättigheter, men så länge de hålls kan konfidentiell information läsas ut eller farligt information skrivas in (t.ex. en annan returadress).

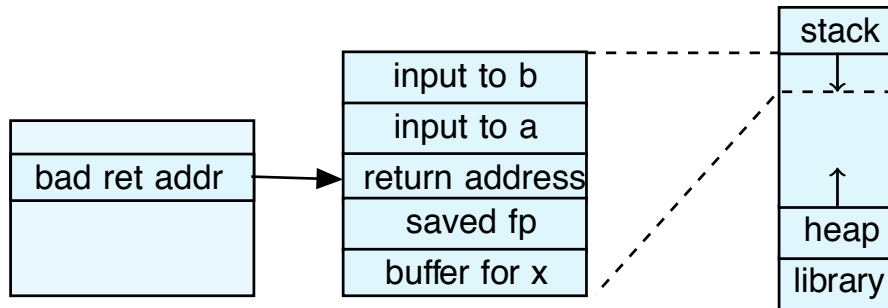
Det går också att accessa arrayen y utanför arraygränserna med liknande möjligheter.

01001001 01000011 01000111

Stack/buffer overrun

Skriv för mycket data i buffern (här x)

I överlappet skrivs data över returadressen eller andra variabler



Demo:
overflow

01001001 01000011 01000111

Tidigt exempel på buffer overrun

"The Morris worm" kom 1988 och infekterade 5-10% av alla datorer kopplade till Internet!

Utnyttjade buffer overrun i deamonen *fingerd* i BSD Unix på VAX-datorer.

Gärningsmannen avslöjades och bötdade \$10000 plus 400 timmar samhällsservice.

pushl \$68732f	push '/sh, <NUL>'
pushl \$6e69622f	push '/bin'
movl sp, r10	save stackp in r10 (string beginning)
pushl \$0	push 0 (arg 3 to execve)
pushl \$0	push 0 (arg 2 to execve)
pushl r10	push string beginning (arg 1 to execve)
pushl \$3	push argc
movl sp, ap	set argv to stackp
chmk \$3b	perform 'execve' kernel call

01001001 01000011 01000111

Tidigt exempel #2 på buffer overrun

I MS/DOS kunde man ha 8 tecken i filnamn och directorynamn.

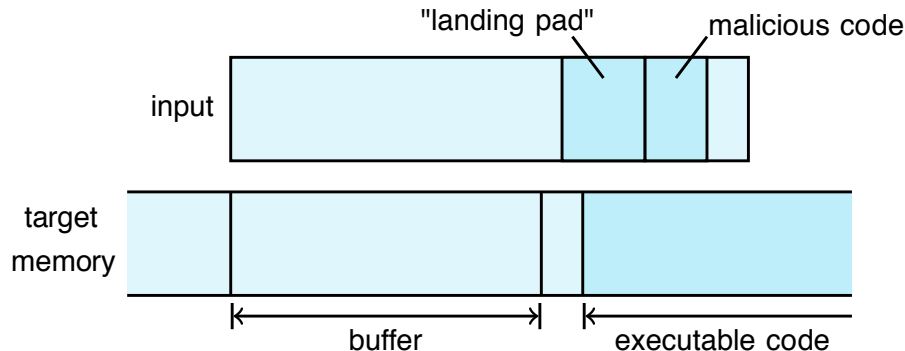
Om man skrev in mer än 8 tecken så... kraschade systemet helt!
Filsystemet blev korrupt och man fick formattera om!
(Availabilityproblem.)

01001001 01000011 01000111

Buffer overruns och "smashing the stack"

Svaghet: Programmerare slarvar ofta med att testa storleken på indatasträngar. Angriparen gör en oväntat lång indata som sedan kan tolkas som exekverbar kod.

Utan kunskap om underliggande program ger detta oftast kracher, men kan också resultera i intrång.



01001001 01000011 01000111

Heap overruns

Svårare att utföra eftersom det är svårt att avgöra var buffern befinner sig relativt målet.

Målet är ofta pekare till öppna filer eller funktioner (givet att heapen innehåller exekverbar kod)

Oftast krascher i stället för intrång, men med många försök (många användare) kan attacken till slut resultera i intrång

01001001 01000011 01000111

Free the mallocs!

Tidigare använt minne kan innehålla information när det allokeras igen.

malloc
tilldela minnet hemlig information
free - nu är det borta! Väl...

malloc görs utan att radera.
Nu innehåller den nya buffern det gamlas värde.

Detta kan även ge läckor vid buffer overrun.

Demo:
dirty-free

01001001 01000011 01000111

Tidigare använt minne - på väggen i Human Fall Flat!



01001001 01000011 01000111

Även på stacken

BILD BORTTAGEN

Samma sak händer på stacken.

En sträng med information läggs på stacken.

När funktionen avslutas "försvinner den".

Nästa funktion får samma minnesarea.

Även ett problem i grafikminnet på GPU:n. Misslyckas en texturladdning så får vi gammal information.

Demo:
dirty-stack

01001001 01000011 01000111

Förebyggande åtgärder: Hårdvara

- Itanium har ett separat register för returadressen.
- Icke exekverbara datablock. AMD kallar detta NX, Microsoft kallar det Data Execution Prevention (DEP), och Intel kallar det eXecution Disable (XD). Kräver stöd av minneshanteraren i CPU:n. DEP introducerades i MS Windows i XP SP2.

01001001 01000011 01000111

Förebyggande åtgärder: Programvara

Icke-exekverbar stack stoppar en del attacker.

Programvara som kräver exekverbar stack slutar fungera.

Förutsägbara minnesaccesser är en fördel för angriparen, därför används stack & heap randomization i alla moderns operativsystem. (Med hur påverkar detta prestandan?)

Stack-based overrun detection (för Visual C++) lägger till tester för korrupt stack vid varje gång en funktion avslutas.

Förebyggande åtgärder: Säkrare funktioner

C är okänt för osäkra strängfunktioner, strcpy, sprintf, getc.

Null-terminerade strängar! Saknas terminering får strängen en okänd längd in i okänt minne! Inget inbyggt test på maxlängd.

T.ex. strncpy innehåller ett argument för maxlängd. Säkrare!

Problem: Säkrare funktioner dåligt standardiserade!

01001001 01000011 01000111

Förebyggande åtgärder: Säkerhet i datatyper

Komplatorer kan testa osäker användning av datatyper, t.ex. att man blandar signed och unsigned.

Dynamisk testning körs i realtid och gör programmet långsammare

Statiskt testning görs vid kompilering. Den är mer komplicerad men kostar inte prestanda.

Vissa språk (Pascal, Java) har strikt testning av datatyper. Andra är släpphänta och tilldelar typer efter användning (JavaScript, Python). Gissa vad som är populärast? :)

Upptäckt

Canaries, minneselement som används för att upptäcka oönskade ändringar i data under exekvering

Kodinspektion för hand är långsamt och du kommer att missa mycket men fungerar ibland.

Automatisk kodinspektion använder sig av expertsystem för att hitta kända svagheter.

Säkerhetstestning med scripts/program som skickar slumpmässiga indata till programmet. Slumpmässiga indata tar tid. Indata fokuseras ofta på förväntade attacker. Bra idé?

Tidigt exempel: "Monkey DA" från Apple.

01001001 01000011 01000111

Begränsa privilegier

Se till att koden inte körs i onödan

Ge inte användare mer rättigheter än de behöver

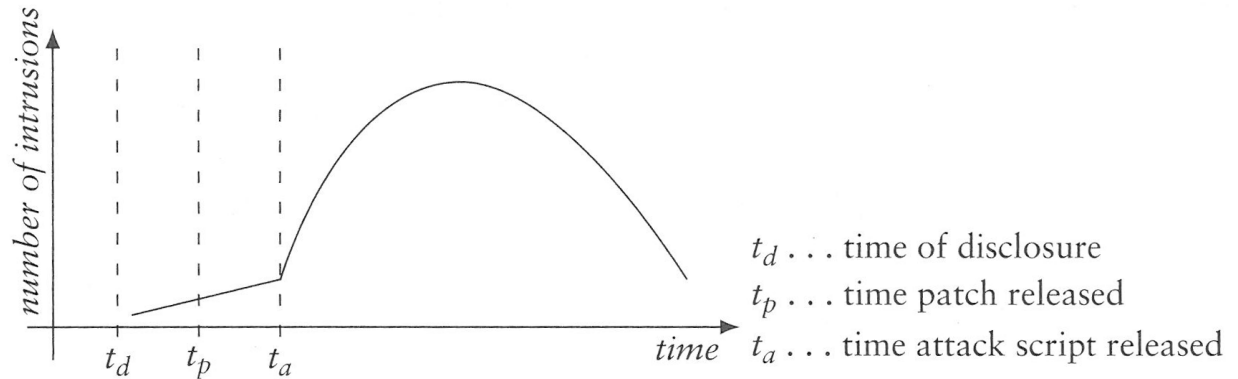
Ta bort rättigheterna snarast möjligt

Aktivera inte funktioner som du inte behöver

01001001 01000011 01000111

Reaktion: Uppdatera

Applicera säkerhetsuppdateringar snabbt.



01001001 01000011 01000111

Bugg-fri programvara?

01001001 01000011 01000111

Testning

Testning görs oftast med *förväntad* användning

Angripare gör oväntade saker

I fältet där du skrev "foo" kommer någon annan att skriva
"supercalifragilisticexpialidocious"!

Jag kunde krascha en Sun-station (Unix) på en minut genom att
skriva en lång rad utan mellanslag i ordbehandlaren!

01001001 01000011 01000111

Buggar

Du vill göra koden bugg-fri (så klart).

Antalet buggar påstås minska med tiden. Det gör det inte.
Varför blir det fler buggar fast vi korrigerar dem hela tiden?

- Nya funktioner, mer och mer komplext
- En korrektion ger upphov till nya fel
- Anpassning till nya standarder - skriv om - gör nya fel
- Ny personal

01001001 01000011 01000111

Ny ingenjör, ny kod...

BILD BORTTAGEN

01001001 01000011 01000111

Ny ingenjör, ny kod...

Mycket vanligt problem.

Komplett nytt system vanligt.

När detta görs på mellannivåer så blir kostnaden stor och ger ofta förlorad funktionalitet och genom att allt skrivs om får man lätt förlorad säkerhet.

01001001 01000011 01000111

Konformism som säkerhetsrisk

BILD BORTTAGEN

"Alla andra gör ju så"

Konformism, att alla gör likadant, gör det lättare för angripare.

Skadlig kod riktar sig oftast mot MS Windows, för det är vanligast och bildar ofta stora monokulturer. Stora angrepp har hänt just i sådana.

Angrip de vanligaste OSen, de vanligaste webbläsarna, de vanligaste verktygen.

Jfr angrepp av skadedjur, sprider sig snabbast i monokulturer.

<https://www.skogsindustrierna.se/hallbarhet/skogsbruk/angreppen-av-granbarkborrar/>

01001001 01000011 01000111

Assurance, Authenticity and Anonymity (AAA)

01001001 01000011 01000111

Assurance, Autenticity and Anonymity (AAA)

Besläktade med CIA men relaterar lite annorlunda till varandra

Assurance: Kan vi lita på att system och människor beter sig som väntat?

Autenticity: Är uppgifter genuina?

Anonymity: Kan uppgifter kopplas till en specifik person?

01001001 01000011 01000111

Assurance

Handlar om att hantera vem/vad vi litar på

Pålitlighet är svårt att mäta

men pålitlighet och hantering av pålitlighet är nödvändigt!

- Kan vi lita på att ett OS är buggfritt?
- Kan datorn lita på att användaren är den den säger sig vara?
- Kan en filmtjänst lita på att du inte kopierar filmen och distribuerar den vidare?
- Kan en dator lita på att den IP-adress den ser är korrekt?

01001001 01000011 01000111

Verktyg för assurance

För att säkra pålitlighet så behöver vi

Policies: Hur förväntar vi oss att användare och system beter sig?

Rättigheter: Vad för aktiviteter har användare och system rätt att göra?

Baserat på detta gör vi säkerhetsmekanismer: System som hanterar rättigheter

01001001 01000011 01000111

Authenticity

Autenticitet handlar om förmågan att avgöra om uppgifter och rättigheter är autentiska, om de är äkta

Inte samma sak som autentisering

Inte heller samma sak som integritet (integriteten hos data i ett system)

01001001 01000011 01000111

Terminologi: Non-repudiation

Repudiation betyder nekande.

Non-repudiation betyder oförmåga att neka att utföra en handling.

Det är skillnad på att säga ja och att inte kunna säga nej.

T.ex. att lämna en uppgift när man inte borde. Systemet vet inte vem som har rättigheterna och saknar spärrar.

Om det inte är möjligt att bevisa att något är äkta eller falskt så skall man inte anta att det är äkta. Äktheten nekas, "is repudiated".

"In general, non-repudiation involves associating actions or changes with a unique individual."

01001001 01000011 01000111

Non-repudiation och accountability

Icke-avvisande och ansvar

Om det blir fel så vill vi kunna spåra vad som hände och vem som gjorde det

Den som gjorde fel skall kunna hållas ansvarig

01001001 01000011 01000111

Verktyg för accountability: Audit trail och digitala signaturer

Audit trail = verifieringskedja

För att avgöra ansvar

Sekundärt mål: För att finna svagheter som möjliggjorde attacken

Ytterligare mål: Hitta och återställa ändringen

Digitala signaturer är ett verktyg för att knyta en person till en uppgift eller handling

01001001 01000011 01000111

Det tredje Aet: Anonymitet

Vår identitet knyts till våra onlineaktiviteter:

- medicinsk dokumentation
- inköp
- juridiska uppgifter
- E-post
- webhistorik

01001001 01000011 01000111

Det tredje Aet: Anonymitet

- Konfidentiell identitet
- Göm innehållet
- Att det finns ett meddelande, vem som var i kontakt med vem
- Analys av datatrafik används för att upptäcka kopplingar mellan personer

"Unlinkability"

01001001 01000011 01000111

Verktyg för anonymitet

- Online: Proxies och VPN. Pålitliga tjänster för att se till att en handling inte kan spåras till en individ.
- Pseudonymer
- Aggregering, kombinerings av data från många individer så sammanräkningen inte kan kopplas till individer

01001001 01000011 01000111

Några fler koncept

01001001 01000011 01000111

Security policy

Regler. Formulering av säkerhetsmålen för en organisation

Vad är det som skall skyddas?

Hur skall detta göra?

För att formulera en "policy" så behöver du veta

- vad som skall skyddas
- hur det kan vara hotat
- vad som hotar
- hur hotet kan hindras

01001001 01000011 01000111

Security policy, exempel på fysisk access

Vem har tillgång till området?

Finns det områden med begränsat tillträde?

Kommer man in med nyckel, kort, vakt...?

Behöver du ha en ID-bricka?

Måste besökare ledsagas?

Kontrolleras väskor vid tillträde?

När låses byggnaden?

Vem har nycklar?

01001001 01000011 01000111

Security policy, exempel på lösenord

Hur långt skall lösenordet vara? ("Max 8 tecken")

Är ASCII-lösenord med enbart gemener tillåtna?

Görs ett test mot ordlista när lösenordet skapas, eller gör systemet detta rutinmässigt?

Hur ofta krävs nytt lösenord?

01001001 01000011 01000111

Terminologi: Hot och STRIDE

Ett hot är en möjlig negativ effekt på tillgångar

Dessa kan kategoriseras, e.g. STRIDE-modellen:

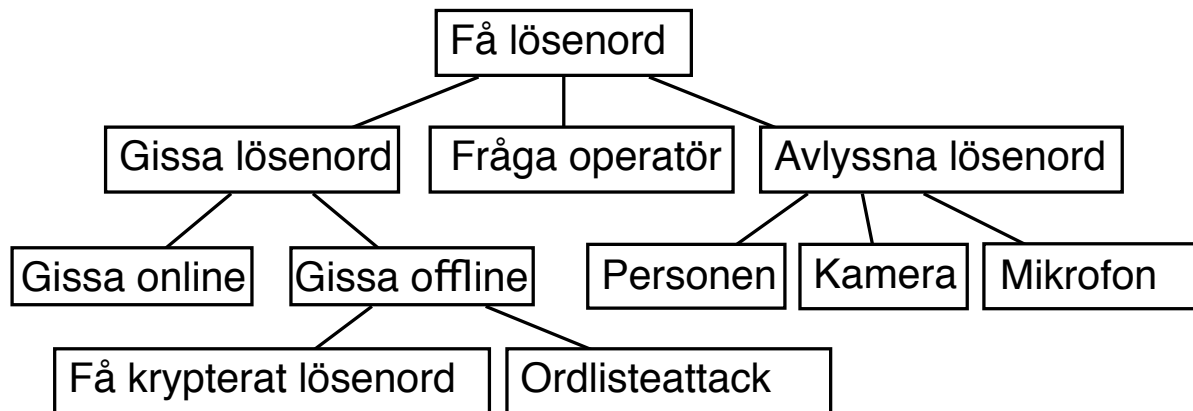
- Spoof identities = Bluffidentiteter
- Tampering with data = Ändringar i data
- Repudiation = Vägran att uppfylla löften/begäran
- Informationsläckor
- DOS, denial of service (inkl DDoS)
- Elevation of privileges = Ökade privilegier

Attacksekvenser

En attack är en sekvens av steg som behövs för att genomföra hotet

Flera attacker kan behövas för att utföra hotet

Attacker är ofta strukturerade som träd:



01001001 01000011 01000111

Angriparens mål och metoder vs CIA

Ekonomisk vinning, ofta C-attacker

Skimming, phishing, industrispionage



För uppmärksamhet, ofta I-attacker

Skriva virus, sabotera websidor etc



Förstöra utrustning, ofta A-attacker

DDoS, systemkrascher etc



01001001 01000011 01000111

Uppföljning

Steget efter åtgärderna.

Hade åtgärderna önskad effekt?

Vad uppskattningarna korrekta?

Behöver strategin korrigeras eller kompletteras?

Har situationen ändrats sedan vi började? Vet vi mer?

01001001 01000011 01000111