

TSIT01 Datasäkerhetsmetoder

Föreläsning 1: Introduktion

Ingemar Ragnemalm

01001001 01000011 01000111

Vilka är vi

Vem är jag?

Universitetslektor, undervisar mest datorgrafik, spelprogrammering och parallellprogrammering

Privat: Hacker (lagliga formen, dvs hobbyprogrammerare), speldesigner, geocachare

Vilka är ni?

Di, tredje året.

Ni kan rätt mycket. Programkod är inget konstigt för er.

01001001 01000011 01000111

Föreläsningsfrågor

1. Varför är datasäkerhet ett växande problem?
2. Vad är en "red hat"?
3. Vad betyder WORM?
4. Varför är IoT ett säkerhetsproblem?
5. Vad innebär 3-2-1-regeln?
6. Varför blev attacken på molntjänsten så fatal?

01001001 01000011 01000111

Denna föreläsning

Kursöversikt

Historik och motivation

Risk och hot

Angriparen

Analys, CIA

Prevention-detection-reaction

Åtgärder

01001001 01000011 01000111

Kursupplägg

- 10 föreläsningar + 2 gästföreläsningar
- En labbkurs
- Ett projekt

Detaljer om labbarna kommer på föreläsning 3

Instruktioner om projekten kommer på föreläsning 2

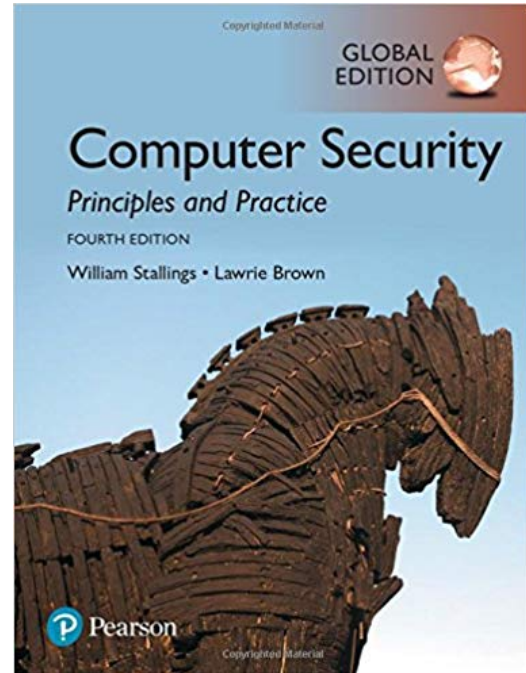
01001001 01000011 01000111

Kursbok

Kursboken är en bra referens som stöd för föreläsningarna. Täcker det mesta av kursen.



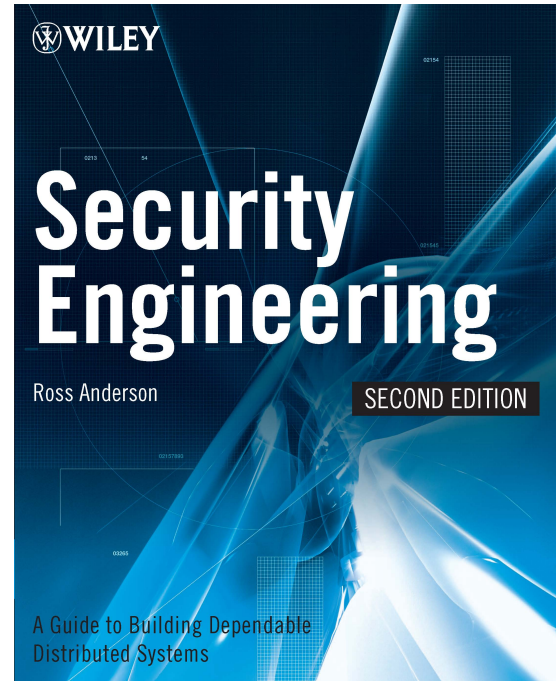
Alternativ: Per Oscarsons "Informations-säkerhet", en lite nättare sak.



01001001 01000011 01000111

Extra kursbok

Tillgänglig gratis online
Täcker ungefär halva kursen.



01001001 01000011 01000111

Organisation

- Ingemar Ragnemalm (Föreläsningar, Examination)
- Guilherme B. Xavier (Föreläsningar)
- Ingo Hölscher (Biometri-föreläsningar)
- Joakim Argillander (Labbar, lektioner)

Ändringar i år: "Återkopplingen" på sista föreläsningen utgår. De muntliga redovisningarna ger motsvarande möjlighet. Läggs om möjligt före jul!

Mina föreläsningar skall om möjligt få "föreläsningsfrågor".

Förra året: Muntlig redovisning infördes på seminarier mot slutet av kursen. Nödvändig åtgärd för att hantera generativ AI!

01001001 01000011 01000111

Kommunikation, kurshemsida

Kurshemsida:

<https://www.icg.isy.liu.se/courses/tsit01/>

E-post

Länkar under

"Organisation"



The screenshot shows the homepage of the TSIT01 Datasäkerhetsmetoder course. The header features a stylized orange head icon and the course title "TSIT01 Datasäkerhetsmetoder" with the subtitle "EN KURS OM SÄKERHET ONLINE". A right-hand sidebar contains a "★ VÄLKOMMEN!" button, a list of navigation links (ORGANISATION, FÖRELÄSNINGAR, LABORATIONER, PROJEKT), a "WORK IN PROGRESS" section with a warning about the page's status for 2022, and a footer note "THIS PAGE IS MAINTAINED BY INGEMAR RAGNEMALM". The main content area welcomes visitors and provides information about the course's focus on data security, its relevance, and its unique design.

TSIT01 Datasäkerhetsmetoder
EN KURS OM SÄKERHET ONLINE

★ VÄLKOMMEN!

ORGANISATION
FÖRELÄSNINGAR
LABORATIONER
PROJEKT

WORK IN PROGRESS

Denna sida är helt ny 2022 och kommer säkert att innehålla inkomplett information och felaktigheter.

THIS PAGE IS MAINTAINED BY
INGEMAR RAGNEMALM

Välkommen till TSIT01 Datasäkerhetsmetoder!

TSIT01 Datasäkerhetsmetoder handlar, som namnet säger, om datasäkerhet, ett ämne som bara blir mer aktuellt ju längre tiden går och vi får fler användare och datalager online.

Denna kurssida är ny för 2022. Notera det orange temat. Kuriosa: Det är faktiskt tematiskt: Kursen handlar om faror, om varningar, så varför inte använda en varningsfärg! Det är lite utmanande att göra det utan att det bli grällt och osmakligt, så jag har gjort mitt bästa för att balansera.

Kurssidans unika utseende är avsiktligt: Du skall alltid veta att du är just på denna kurssidan!

[Officiell kursplan](#)

01001001 01000011 01000111

9(75)

Lärandemål

- Förstå och tillämpa målen med datasäkerhetsarbete
- Kunna analysera situationer ur säkerhetssynpunkt.
- Välja rätt åtgärder och utvärdera dem.

I detta ingår autenticering, verktyg för nätverkssäkerhet (speciellt "pentesting") och kryptering

Vad examineras?

- Laborationer som övar "pentesting"
- Utför en analys *systematiskt*, med åtgärder. Redovisas muntligt och skriftligt.

01001001 01000011 01000111

**Varför behöver vi bry
oss om datasäkerhet?**

01001001 01000011 01000111

Varför behöver vi bry oss om datasäkerhet?

Det blir allt svårare att se till att data är fysiskt isolerat.

Allt är ihopkopplat och därmed nåbart.

Möjligheterna är stora, och därmed även möjligheterna till missbruk.



01001001 01000011 01000111

Exempel: Extremt skadliga krypteringsattacker!

CRITICAL CONDITION —

**Patient dies after ransomware attack
reroutes her to remote hospital**

**Outage caused an hour delay in treatment for woman
with life-threatening condition.**

[Dan Goodin](#) - 9/17/2020, 10:06 PM

<https://arstechnica.com/information-technology/2020/09/patient-dies-after-ransomware-attack-reroutes-her-to-remote-hospital/>

01001001 01000011 01000111

Ett annat exempel: IoT-botnet

BILD BORTTAGEN

01001001 01000011 01000111

Kritisk infrastruktur (availability)

BILD BORTTAGEN

01001001 01000011 01000111

**[Best of 2019] NATO CCDCOE strategist: Die Hard 4
is the perfect way to describe real cyberwarfare**

BILD BORTTAGEN

01001001 01000011 01000111

Den grymma verkligheten i cyberbrottslighet

Tid mellan varje attack mot en oskyddad dator: 39 sekunder

Uppskattad kostnad för cyberbrott i 2019: \$ 2 triljoner
(Amerikanska, dvs miljarder)

Anektot: Min egen webserver

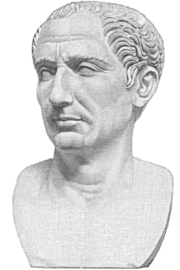
BILD BORTTAGEN

01001001 01000011 01000111

Lite historik

01001001 01000011 01000111

Innan 1960-talet, informationssäkerhet



Ända sedan antiken! Gömda meddelanden, Caesar-chiffer...

Mest militära tillämpningar

Kryptomaskiner: Enigma, 20-tal, andra världskriget

Säkerhet = kommunikationssäkerhet

Säkerhet = Stark kryptering



01001001 01000011 01000111

1960-1980-tal

BILD BORTTAGEN

I media: kryptomaskinen "Lektor" i
"From Russia with love", 1963.

1971, första viruset/masken Creeper.

1982, Elk Cloner, spreds via disketter.

1989, WDEF-viruset, spreds via nedladdade program från FTP-arkiv

1978 grundades SECTRA i Linköping. Denna kursen startades 1979
(7:e november i S19 enligt Viiveke Fåk som höll kursen många år)!

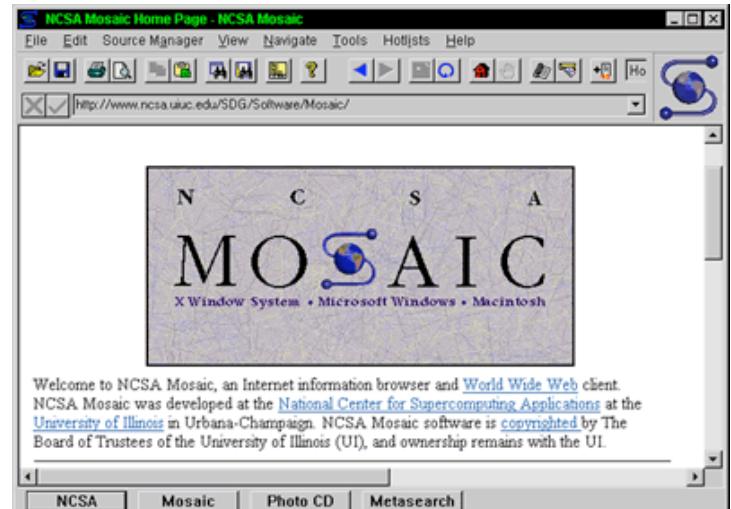
Kryptering fortfarande huvudämnet men virus hade kommit.

01001001 01000011 01000111

1990-talet, Internet-åldern

Denial-of-service-attacker
förekommer

Mer tidiga virus, mest bus,
utnyttjade uppenbara
säkerhetshål



01001001 01000011 01000111

2000-talet —webåldern

Samma teknik som 90-talet men mycket fler användare

Mer kommersiella tillämpningar

SQL injection, cross-site scripting, DNS-attacker

Kriminella upptäcker nätet

Mycket fler diskreta attacker

Större ekonomiska förluster

BILD BORTTAGEN

01001001 01000011 01000111

2010-talet — cloud och stora sociala nätverk

Onlinelagring och online-kommunikation för att accessa egna data. Din information är inte längre lokalt på din disk.

Sociala nätverk är stora. Nya frågor om säkerhet och integritet i dessa.

BILD BORTTAGEN

01001001 01000011 01000111

2010-talet — Internet of Things

Smartphones lagrar allt om våra liv

Våra apparater vet allt om oss -
privacy, integritet

Fler och fler apparater är online -
Internet of Things

Kan någon styra mina apparater?

Kan någon stänga av mitt larm?

Biltillverkare fuskar med
programvara (Dieselgate)

Myndigheters övervaknings-
system (Snowden)

Bitcoins, kryptovalutor

Ransomware-trojaner
(Cryptolocker, Cryptowall)

01001001 01000011 01000111

Your files are encrypted.

To get the key to decrypt files you have to pay **750 USD/EUR**. If payment is not made before **00:00:00** the cost of decrypting files will increase **2** times and will be **1500 USD/EUR**

Prior to increasing the amount left:

42h 48m 35s

Your system: **Windows 7 (x64)** First connect IP: **192.168.1.1**  Total encrypted **10** files.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?



1. You should register Bitcon wallet ([click here for more information with pictures](#))
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

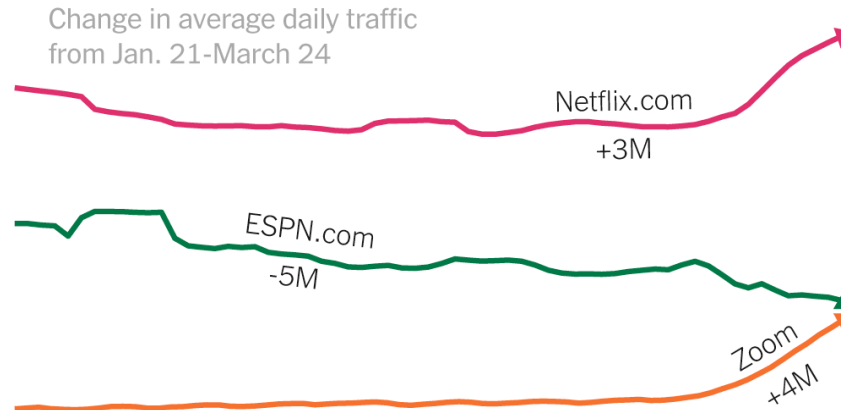
[1](#) [2](#) [3](#) [4](#) [5](#) [6](#)

01001001 01000011 01000111

2020-talet — Den nya vardagen?

Covid-19 har tvingat fram mer jobb från hemmakontor
(Speciellt i teknik- och finansområdena)

Strömningstjänster dominerar allt mer!



01001001 01000011 01000111

2020-talet — Generativ AI

Generativ AI blir allt starkare.

BILD BORTTAGEN

Tillgång: Verktyg för att skapa bilder från text, och för att skapa texter.

Problem: Kan användas för fusk och förfalskningar. Lättare att förfalska information. Deepfakes, falska videos, falska ljudspår. Integritetsproblem. Kan användas för politiska ändamål, för att påverka aktiekurser...

01001001 01000011 01000111

Översikt över ämnet

01001001 01000011 01000111

Ämnet datasäkerhet

Datasäkerhet handlar om att hindra och upptäcka oauktoriserade handlingar av användare av ett datorsystem.

Datasäkerhet arbetar med åtgärder vi kan göra för att hindra och hantera oönskade handlingar, speciellt avsiktliga.

Översikt

Risk och hot

Typer av angripare

Analys och hantering, prevention-detection-reaction, CIA, åtgärder

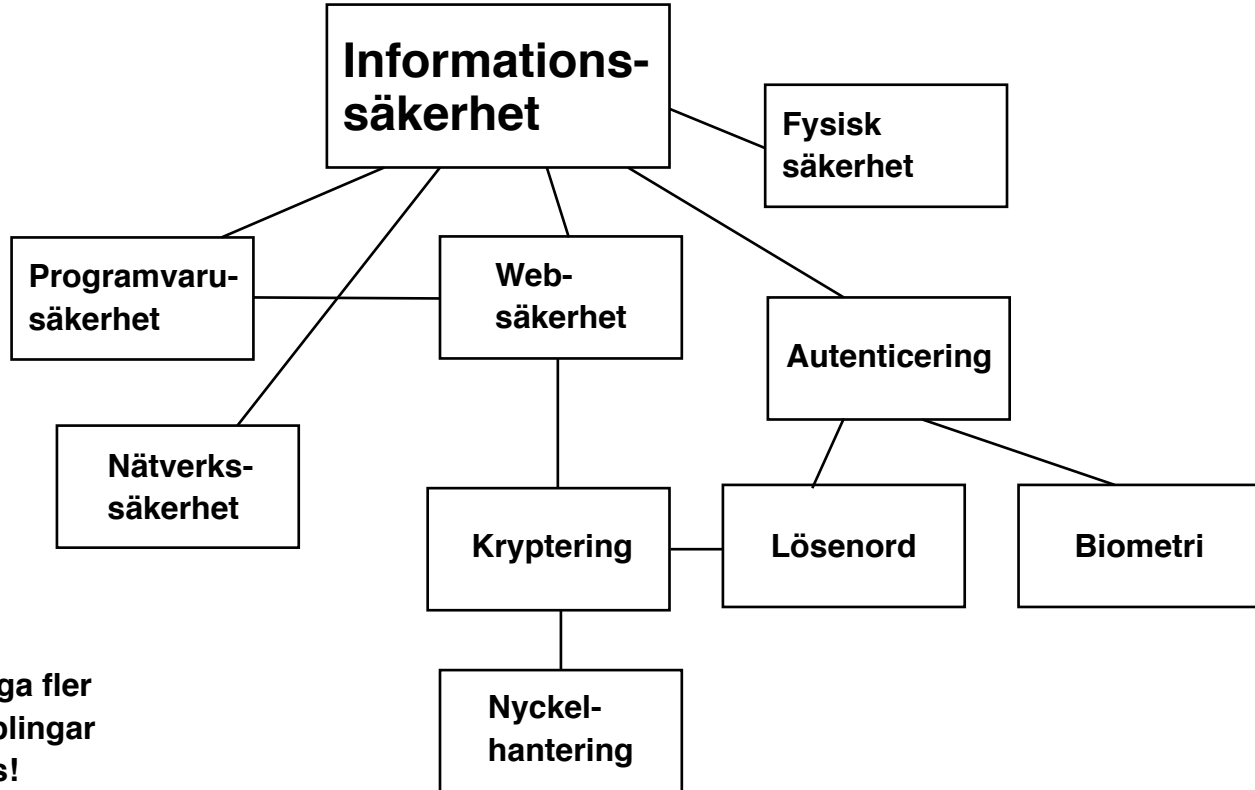
Intrång genom lösenord, avlyssning, social engineering

Webbattacker

Programvaruattacker

Autenticering, kryptering, biometri

01001001 01000011 01000111



Många fler
kopplingar
finns!

01001001 01000011 01000111

Analysera säkerhet metodiskt, översiktlig kedja

- Vad är situationen, översiktligt?
- CIA, gå igenom situationen från flera aspekter
- Identifiera risk, hot, angripare
- Riskanalys, hur troligt, hur farligt?
- Vad kostar åtgärderna?
- Åtgärder med prioritering enligt riskanalysen, uppdelat i prevention - detection - reaction

Vi skall nu gå igenom dessa delar

01001001 01000011 01000111

Risk och hot

01001001 01000011 01000111

Hotagenter, tillgångar

Säkerhet baseras på tillgångar som behöver skyddas.

Dessa hotas av *hotagenter, threat agents*.

Mellan dessa står skyddet, säkerhetsåtgärderna,
controls.

01001001 01000011 01000111

Vad är en *risk*?

Risk = sannolikhet för ett problem * skadan.

Risken är dels hur troligt ett intrång är och dels hur mycket skada det kan göra.

Svårt att kvantifiera, men alla uppskattar det dagligen.

Exempel: Går du över gatan om du ser en bil en bit bort som rör sig mot dig?

Vad är en *risk*?

Risk = sannolikhet för ett problem * skadan.

Risken är dels hur troligt ett intrång är och dels hur mycket skada det kan göra.

Svårt att kvantifiera, men alla uppskattar det dagligen.

Exempel: Går du över gatan om du ser en bil en bit bort som rör sig mot dig?

Ändras detta om du bär på ett litet barn?

01001001 01000011 01000111

Vad är en *risk*?

Risk = sannolikhet för ett problem * skadan.

Risken är dels hur troligt ett intrång är och dels hur mycket skada det kan göra.

Svårt att kvantifiera, men alla uppskattar det dagligen.

Exempel: Går du över gatan om du ser en bil en bit bort som rör sig mot dig?

Ändras detta om du bär på ett litet barn?

Detta är ett exempel på *risk acceptance*

01001001 01000011 01000111

Vad är en *risk*?

Fråga: Hur mycket är det värt för dig?

Om svaret är ett positivt tal, då har det också värde för någon annan.

01001001 01000011 01000111

Risk

Risken påverkas av hotet, säkerhetsåtgärderna och tillgångarna.

Sannolikheten ges av hotet och säkerhetsåtgärderma.

Skadan ges av tillgångens värde.

01001001 01000011 01000111

Angriparen

01001001 01000011 01000111

Angripare

Typer av angripare:

- Insiders, någon som har interna kunskaper
- Externa individer, små resurser, ofta låga kunskaper
- Statligt sponsrade organisationer, stora resurser, stora kunskaper

01001001 01000011 01000111

Angripare

Angriparens mål:

- Databrottslingar, cyber criminals: Brottslingar med finansiella mål.
- Aktivister: Ofta grupper. Angripare med sociala eller politiska mål. Kallas också "hacktivister". T.ex. Anonymous och LulzSec, Chelsea Manning och Edward Snowden.
- Spionage eller sabotage. Avslöjad information (i.e. Snowden) visar att detta utförs av en betydande mängd länder. Det genererar också inkomst för vissa (i.e. Nordkorea).
- Angripare med andra motiv än de ovan, som teknisk utmaning eller status och rykte inom någon grupp.

01001001 01000011 01000111

Angriparnas kompetensnivåer

- Nybörjare/lärling (apprentice). Angripare med låg kompetens använder primärt existerande verktyg. *Detta är majoriteten av angripare.* Även kända som "script-kiddies".
- Medelgod (gesäll, journeyman): Angripare med tillräckliga tekniska kunskaper för att modifiera och bygga ut existerande verktyg för att utnyttja nyupptäckta säkerhetshål eller för att fokusera på andra målgrupper.
- Mästare/expert: Angripare med stora kunskaper förmögna att upptäcka nya säkerhetshål eller skriva nya attackverktyg. Många av dessa är anställda av statliga organisationer.

Angripare

Hacker betydde från början "fixare", någon som kunde meka med maskiner utan att vara formell expert. I datorsammanhang kom det att betyda entusiaster som mekade och hobbyprogrammerade datorer.

Filmen WarGames (1983) använde ordet hacker på ett sätt som för tittaren såg det som ordet för databrottsling. Efter detta har ordet fått en negativ ton. Hackers (entusiasterna alltså) introducerade ordet "crackers" för databrottslingar men det har inte slagit igenom.

Numera skiljer man på *white hat* och *black hat* hackers.

01001001 01000011 01000111

Hatten är din



White hat: Legitima syften, förbättrar säkerhet

BILD BORTTAGEN



Black hat: Databrottslingar, illegitima syften

Fler "hattar" har definierats:



Grey hat: angriper utan personlig vinning



Green hat: nybörjare, lär sig, utgör sällan hot.



Blue hat: aggressiva, ofta ute efter hämnd



Red hat: målet är att skydda genom att angripa black hat

Viss förvirring
förekommer,
t.ex om blue
hat.

01001001 01000011 01000111

Enkelt "red hat"-exempel

Historia som cirkulerar på internet. Skröna?

Script kiddie skryter med att den kan slå ut vilken dator som helst bara den har IP-adressen.

Red Hat utmanar:

- Kan du slå ut min?
- Visst! Vad är din IP-adress?
- 127.0.0.1

Smack! Fick dig!

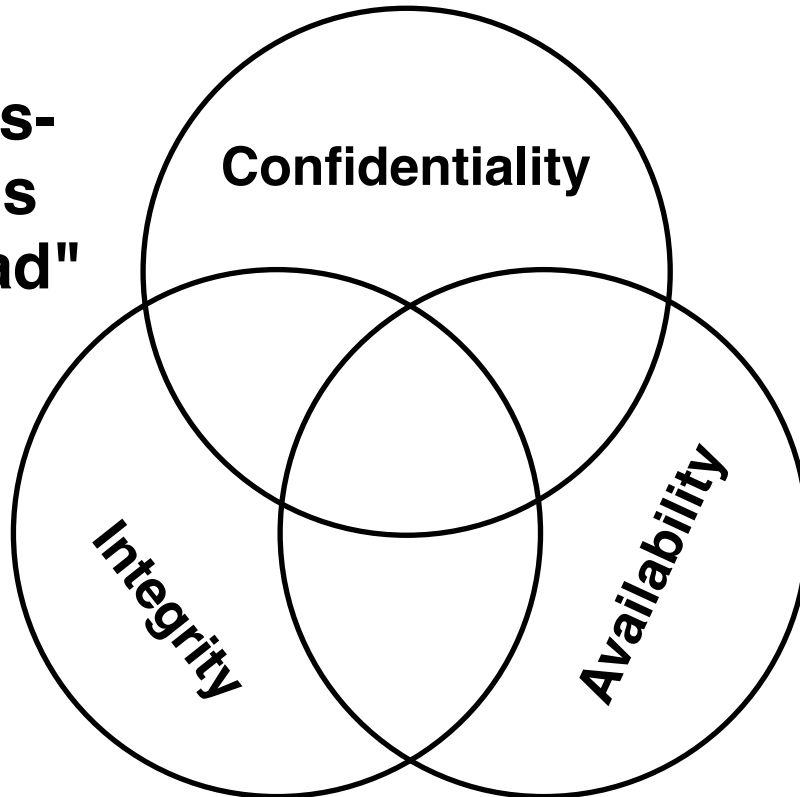
<https://gist.github.com/taq/5793430>

01001001 01000011 01000111

CIA: Confidentiality, Integrity and Availability

01001001 01000011 01000111

Informations- säkerhetens centrala "triad"



På svenska: KRT
Konfidentialitet
Riktighet
Tillgänglighet

01001001 01000011 01000111

Analys: CIA

Confidentiality: Bara auktoriserade personer får ta del av informationen

Integrity: Bara auktoriserade personer får ändra informationen

Availability: Auktoriserade personer ges möjlighet att läsa och ändra informationen

Oscarson kallar detta KRT: Konfidentialitet, riktighet, tillgänglighet. (Jag föredrar KIT, konfidentialitet, integritet, tillgänglighet.)

01001001 01000011 01000111

Analys: CIA

CIA är en kategorisering för analysen! Använd denna för att analysera problemet.

Åtgärder kommer sedan.

01001001 01000011 01000111

Analys: Confidentiality (konfidentialitet)

Hindra oauktoriserade personer från att läsa känslig information

Kan betyda att dölja informationen, men också att dölja att informationen existerar

RISK: Att värdefull konfidentiell information nås av obehöriga.

01001001 01000011 01000111

Analys: Integrity (riktighet)

Vi vill hindra oauktoriserade från att ändra känsliga data,
eller att den ändras av misstag

Exempel på hur svårt det kan vara: "viskleken"

01001001 01000011 01000111

Analys: Availability (tillgänglighet)

ISO7498-2: "The property of being accessible and usable upon demand by an authorized entity"

I grund och botten, hindra denial-of-service, eller hindra att data förloras

Handlar inte om att data enbart skall vara åtkomlig för auktoriserade, för det är C+I (konfidentialitet och integritet)

01001001 01000011 01000111

Sök åtgärder: Prevention - detection - reaction

01001001 01000011 01000111

Åtgärder: Prevention - detection - reaction

Prevention (hindra) försöker hindra skador på dina tillgångar

Detta kan vara kryptering, brandväggar...

Detection (upptäcka) försöker upptäcka skador, hur skadan har skett, vem som orsakade skadan

Typiska verktyg är Intrusion Detection Systems (IDSs), digitala signaturer mm. Exempel: Du får en varning om du loggar in på ny dator!

Kan också användas för att se att en attack pågår

Reaction (reaktion) försöker reparera skadan, återskapa tillgångar, och förbättra existerande skydd

01001001 01000011 01000111

Exempel: Prevention - detection - reaction

Prevention vill hindra skador på tillgångar

Använd inte kortnummer öppet online. Använd kryptering när du beställer saker med kreditkortsnummer.

Säljaren utför tester (t.ex. leveransadress). Exempel: Min chef beställde en produkt och ville ha den levererad hem till mig. Det gick inte! (False positive.)

01001001 01000011 01000111

Exempel: Prevention - detection - reaction

Detection försöker upptäcka skador, hur skadan har skett, vem som orsakade skadan

En transaktion som du inte beordrat dyker upp i din transaktionslista

Mängden pengar och platsen pengarna drogs från (leveransadress) kan användas för att spåra brottslingen

01001001 01000011 01000111

Exempel: Prevention - detection - reaction

Reaction (reaktion) försöker reparera skadan, återskapa tillgångar, och förbättra existerande skydd

Installera data från backupen

Rapportera händelsen, spärra kortet

Kostnaden kan täckas av kortinnehavaren, säljaren eller banken beroende på orsaken till intrånget

Sluta använda kort i okrypterade kanaler!

01001001 01000011 01000111

Åtgärder

Vi har avgjort vilka typer av problem vi har och hur vi kategoriserar åtgärder.

Låt oss nu gå igenom konkreta åtgärder!

01001001 01000011 01000111

Åtgärder för konfidentialitet

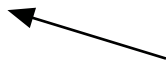
Fysiskt begränsat tillträde

Hinder för stöld av utrustning (larm)

Tillträdeskontroll (inloggning) i datorsystem

Krypterad kommunikation och lagring

Felfria, buggfria program



Sagt av någon som inte
programmerar?

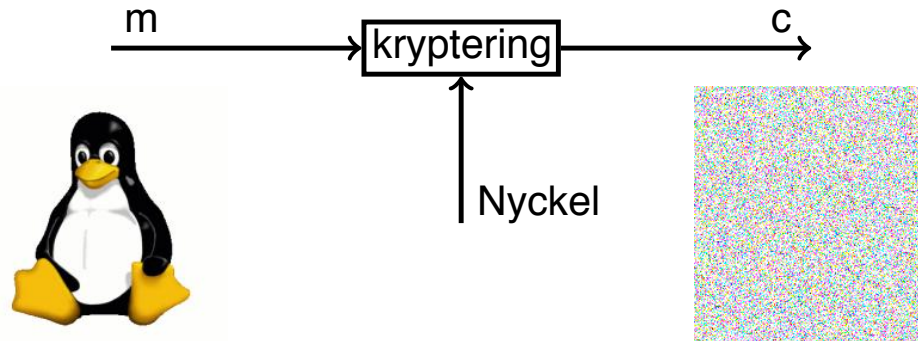
01001001 01000011 01000111

Åtgärder för konfidentialitet: Kryptering

Ett meddelande krypteras med en nyckel

Meddelandet hålls hemligt för alla som inte har nyckeln

Det finns varianter där alla kan kryptera men bara en kan dekryptera

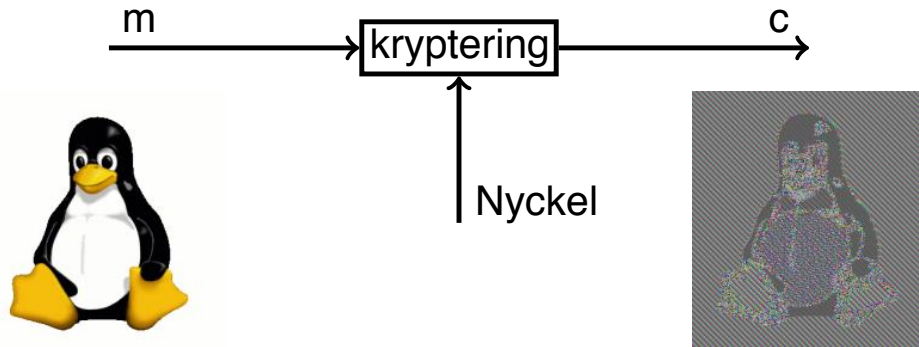


01001001 01000011 01000111

Åtgärder för konfidentialitet: Kryptering

Bra kryptering döljer all information.

Dålig kryptering kan gå att knäcka eller släpper igenom värdefull information.



01001001 01000011 01000111

Åtgärder för integritet

Två delar:

- Metoder för att hindra ändringar och säkra kopior av oförändrad information
- Metoder för att kontrollera att informationen är korrekt

01001001 01000011 01000111

Åtgärder för integritet

Hindra ändringar:

Fysiskt begränsat tillträde

Tillträdeskontroll (inloggning) i datorsystem

Skydd mot ändringar kräver starkare, kryptografiska verktyg

Backuper för att återställa data, speciellt i permanent minne, WORM-backuper. (Säkrar även tillgängligheten.)

01001001 01000011 01000111

BILD BORTTAGEN

01001001 01000011 01000111

Backup svårare än man kan tro

Vi vill också hindra dataförlust från olyckor.

Exempel: Diskpacke-olyckan.
(Lär ha hänt med ett DATASAAB-system.)

Läsning från diskpacken misslyckas.

Operatören tar backupen och sätter den i *samma läsare* -
som genast förstör även backupen för problemet var
kraschat läshuvud!

När vi måste gå tillbaka till backupen, var försiktig med den!



01001001 01000011 01000111

Backup svårare än man kan tro

Aktuellt fall (augusti förra året):

ComputerSweden

BRANSCH EVENT WHITEPAPERS NYHETSREV

MOLNET 2023-08-24 10:59

Danska molnföretag utslagna av cyberattack

Attacken mot Cloudnordic och Azerocloud drabbar hundratals danska företag.

De hade bara EN backup och den var on-line och förstördes samtidigt!

01001001 01000011 01000111

Backup svårare än man kan tro

3-2-1-regeln för backuper

Ha TRE kopior av viktiga data

Använd minst TVÅ olika media

Ha minst EN på annan plats.

Det finns varianter av detta.

Det är inget fel på din molnbackup, eller din lokala hårddisk, etc, men ha EN TILL.

Besläktad regel: En skall alltid finnas som inte är online!

01001001 01000011 01000111

Åtgärder för integritet

Verifiera att informationen är korrekt:

Historiskt: Permanent bläck, signering, sigill, stämplor

Checksummor: Värden som verifierar att data är oförändrad, inklusive transmissionfel och mediafel, även *felrättning* (ex: SARABAND). Felrättning ger både integritet med verifiering och tillgänglighet.



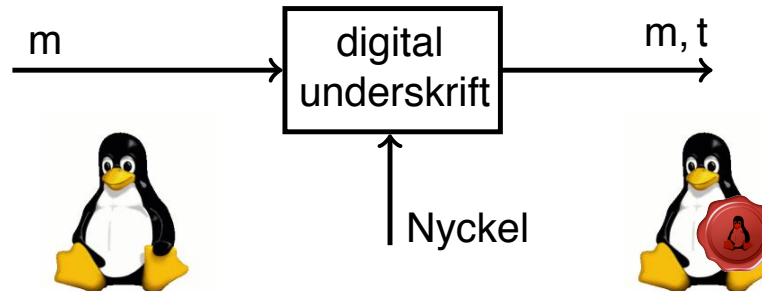
01001001 01000011 01000111

Kryptografiska verktyg för integritet

Digital signatur, auktoriseringskod, skapas med en nyckel

Integritet testas genom att upptäcka ändringar i lagrad eller överförd data genom att jämföra verifikationskoden med originalet

Tanken är att det skall vara svårt att skapa verifikation utan en nyckel



01001001 01000011 01000111

Konfidentialitet och integritet

Konfidentialitet och integritet baseras ofta på samma teknik

Hindra access till fysiskt medium

Accesskontroll på alla logiska datavägar

Kryptografiteknik

Åtgärder för tillgänglighet

Skydd mot fysiska hot och attacker

Säker kraftförsörjning

Brandskydd

Översvämningsskydd

Kontrollerad temperatur och luftfuktighet

Stormtåliga byggnader

Skydd mot skador från attacker (inkl olyckor) på dataintegritet

Backupar, backupar, backupar!

01001001 01000011 01000111

Åtgärder för tillgänglighet

Åtgärder mot överbelastning

Redundans i servrar och diskar

Utrustning som kan upptäcka och förhindra DOS-attacker

Åtgärder mot systemkrascher

Testa alla indata mot ogiltiga värden

Slå av oanvända funktioner

Installera uppdateringar (men med försiktighet!)

01001001 01000011 01000111

Konfidentialitet och tillgänglighet är knepigt

BILD BORTTAGEN

01001001 01000011 01000111

**CIA är ett centralt koncept
som ni bör använda i era
rapporter!**

Tips: CIA-analys först, sedan
åtgärder!

01001001 01000011 01000111