TSIT01 Datasäkerhetsmetoder

Föreläsning 1: Introduktion

Ingemar Ragnemalm

RENSAD PÅ COPYRIGHTADE BILDER

01001001 01000011 01000111

Vilka är vi?

Vilka är ni?

Di, tredje året. Examen närmar sig!

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

Vem är jag?

Universitetslektor, undervisar mest datorgrafik, spelprogrammering och parallellprogrammering

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

Denna föreläsning

Kursöversikt

Historik och motivation

Risk och hot

Angriparen

Analys, CIA

Prevention-detection-reaction, åtgärder

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?

Kursupplägg

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

Detaljer om labbarna kommer på föreläsning 3

Instruktioner om projekten kommer på föreläsning 2

Kursbok

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

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

Extra kursbok

Tillgänglig gratis online
Täcker ungefär halva kursen.

Organisation

- Ingemar Ragnemalm (Föreläsningar, examinator)
- Ingo Hölscher (Biometri-föreläsningar)
- Martin Clason, Supratim Manna, Mahyar Mohammadi (Labbar)
- (Ej bestämt vem) Presentationer

Nyheter

Ovanligt mycket!

Ändringar i år:
- En dugga till (tre i stället för två)
- Vissa labbar skall redovisas muntligt.
- Jag tar över fler föreläsningar.

Förra året: Nytt labbsystem, duggor infördes, rapporten reviderad och mindre del av examinationen. Rapporterna baseras på presentationerna.

Kommunikation, kurshemsida

Kurshemsida:

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

E-post:

Länkar under

"Organisation"



Lärandemål

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

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

Vad examineras?

- Laborationer som övar "pentesting"
- Analysera ett fall. Redovisas muntligt och skriftligt.
- Duggor. (Viktigt! De är en stor del av betyget!)

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/

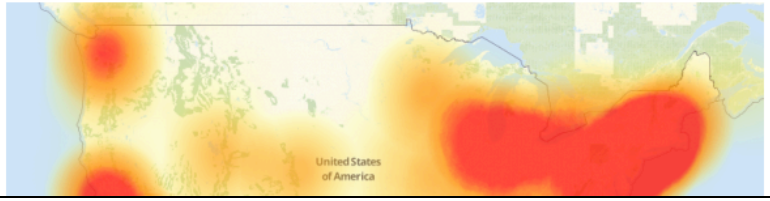
Ett annat exempel: IoT-botnet

KrebsonSecurity
In-depth security news and investigation

21 OCT 16 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



Kritisk infrastruktur (availability)

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

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 biljoner)

Anektot: Min egen webserver

DDoS-attack 2024



Två gripna efter hackerattacken mot Verisure

LINKÖPING

Två personer har gripits och anhållits efter den misstänkta hackerattacken mot larmföretaget Verisure, med huvudkontor i Linköping.

Just nu pågår en förundersökning om grovt dataintrång och försök till grov utpressning kopplad till det misstänkta cyberangreppet som Verisure utsatts för. Kammaråklagare Sandra Helgadottir vid Riksenheten mot internationell och organiserad brottslighet har åtagit sig att leda förundersökningen som sådan kan jag inte gå in på några detaljer. Det har att göra med att vi befinner oss i ett känsligt läge och att det råder förundersökningssekretess, säger Helgadottir.

Vad var det som ledde fram till gripandet?

– Det är inga detaljer som jag kan gå in på i nuläget, tyvärr.

Sandra Helgadottir uppger också att hon inte kan gå in på detaljer kring de misstänkta, exempelvis gällande kön och ålder.

När väntas beslut om häktning?

– Jag måste gå in till tingsrätten med en framställan om häktning senast på torsdag klockan 12.

Det var i slutet av förra veckan som det blev känt att Verisure hade utsatts för ett cyberangrepp.

"Vi upptäckte nyligen obehörig åtkomst av en tredje part gällande data relaterat till Alert Alarm som lagras hos en extern faktureringspartner. Vi arbetar för tillfället med att utreda incidenten tillsammans med våra expertrådgivare och har meddelat polisen samt relevanta myndigheter", skrev företaget till TT då, för att ge en lägesbild av vad som hänt.

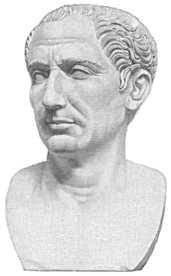
Annie Hogner

Corren
2024-10-25

01001001 01000011 01000111

Lite historik

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



1960-1980-tal

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

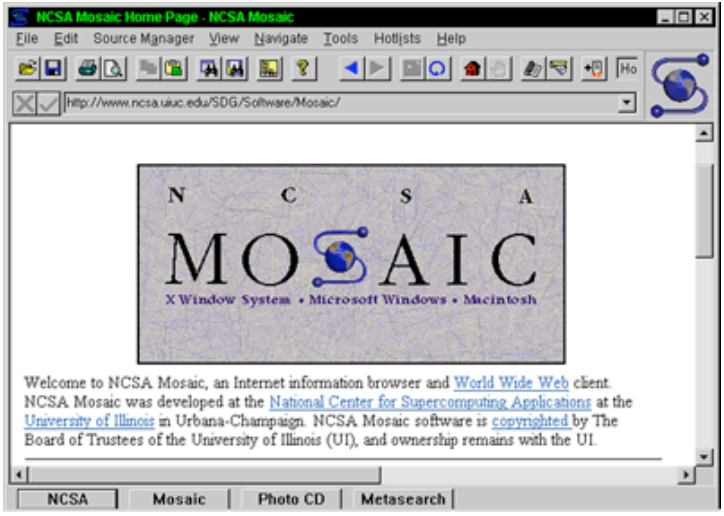
1978 grundades SECTRA i Linköping. Denna kursen startades 1979 (7:e november i S19 enligt Viiveke Fåk som höll kursen många år)!

Kryptering fortfarande huvudämnet men virus hade kommit.

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

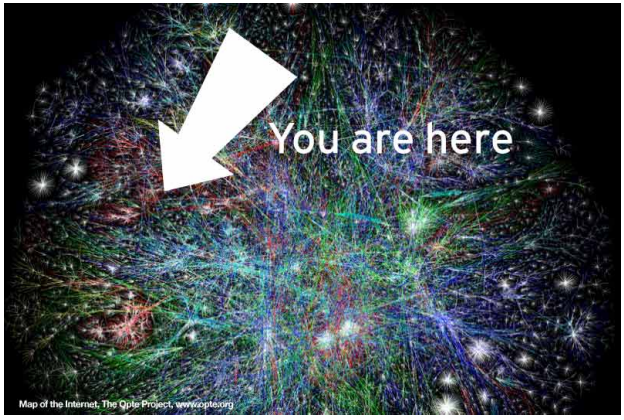
Mer kommersiella tillämpningar

SQL injection, cross-site scriptning, DNS-attacker

Kriminella upptäcker nätet

Mycket fler diskreta attacker

Större ekonomiska förluster

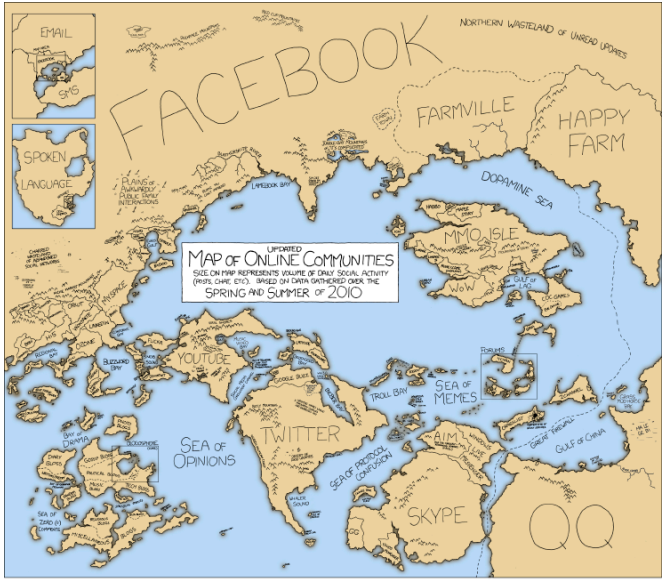


01001001 01000011 01000111

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.



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

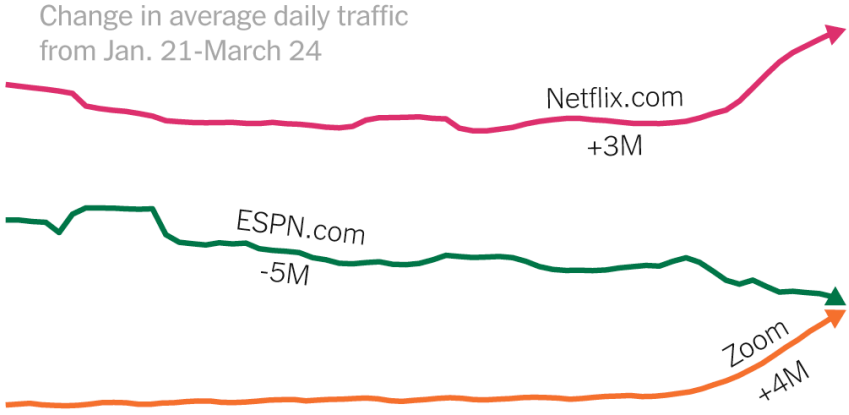


01001001 01000011 01000111

2020-talet — Den nya vardagen?

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

Strömningsstjänster dominerar allt mer!



01001001 01000011 01000111

2020-talet — Generativ AI

Generativ AI blir allt starkare.

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...

Översikt över ämnet

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.

Också viktigt: Prioriteringar!

Översikt

Risk och hot

Typer av angripare

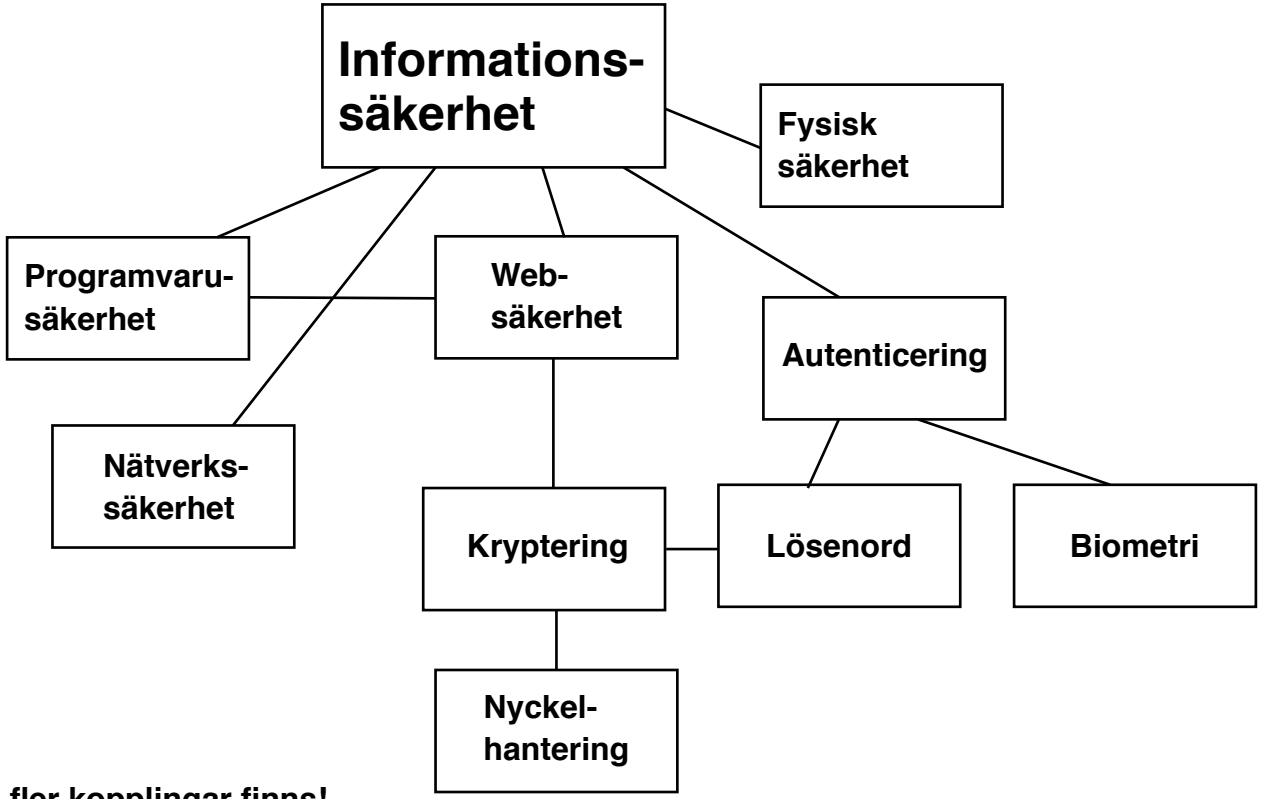
Analys och hantering, CIA, åtgärder: prevention-detection-reaction

Intrång genom lösenord, avlyssning, social engineering

Webattacker

Programvaruattacker

Autenticering, kryptering, biometri



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

Risk och hot

Hotagenter, tillgångar

Säkerhet baseras på tillgångar som behöver skyddas.

Dessa hotas av *hotagenter, threat agents*.

Mellan dessa står skyddet, säkerhetsåtgärderna, *controls*.

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?

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*

Risk

Risken påverkas av hotet, säkerhetsåtgärderna och tillgångarna.

Sannolikheten ges av hotet och säkerhetsåtgärderma.

Skadan ges av tillgångens värde.

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

Angripare

Angriparens mål:

• Databrottslingar, cyber criminals: Brottslingar med finansiella mål.

• Aktivister: Ofta grupper. Angripare med sociala eller politiska mål. Kallas också "hacktivister".

• Spionage eller sabotage.

• Angripare med andra motiv än de ovan, bus eller status.

Angriparnas kompetensnivåer

• Nybörjare/lärling (apprentice). Angripare med låg kompetens använder primärt existerande verktyg, "script-kiddies".

• Medelgod (gesäll, journeyman): Kan modifiera och bygga ut existerande verktyg.

• Mästare/expert: Angripare med stora kunskaper. Upptäcker säkerhetshål, skriver nya attackvektyg. Ofta anställda av statliga organisationer.

Angripare

Hacker betydde från början "fixare".

Filmen WarGames (1983) -> databrottsling.

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

Hatten är din


White hat: Legitima syften, förbättrar säkerhet


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

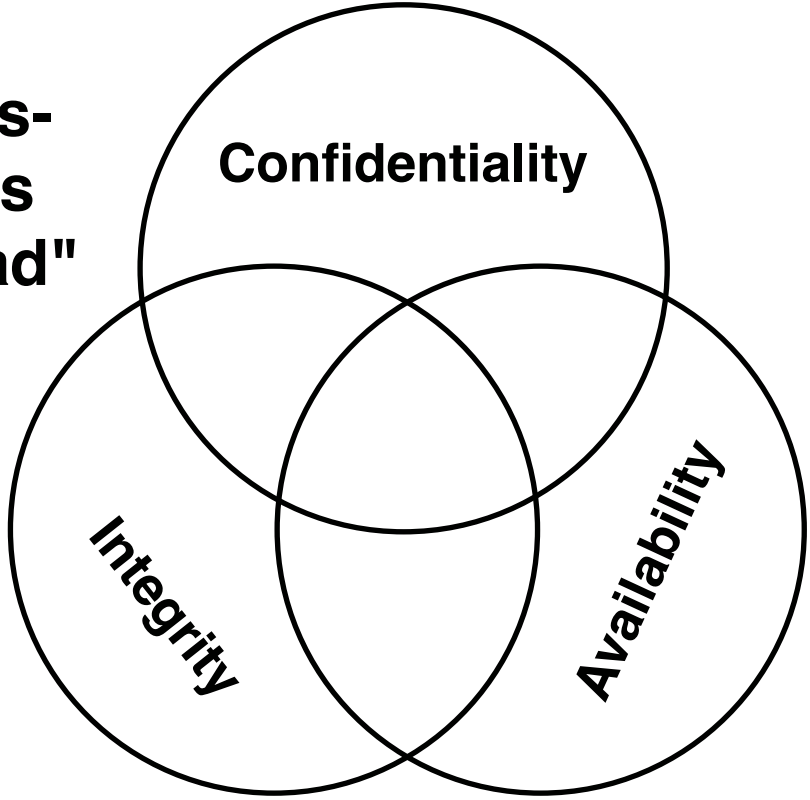
Smack! Fick dig!

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

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 kommma åt/se X

Integrity: Bara auktoriserade personer får ändra/flytta X

Availability: Kommer verkligen auktoriserade personer åt X?

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

Analys: CIA

CIA är en kategorisering för analysen! Används för att analysera problemet.

Åtgärder kommer sedan.

Analys: Confidentiality (konfidentialitet)

Hindra oauktoriserade personer från att komma åt/se X

Kan betyda att hindra att man kommer åt X, men också att dölja att X existerar

RISK: Att hemliga X nås av obehöriga.

Analys: Integrity (riktighet)

Vi vill hindra oauktoriserade från att ändra/ta bort X, eller att det görs misstag

Är information korrekt? Exempel på hur svårt det kan vara: "viskleken"

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)

Sök åtgärder: Prevention - detection - reaction

Åtgärder: Prevention - detection - reaction

Prevention (hindra): hindra skador på dina tillgångar

Kryptering, brandväggar...

Detection (upptäcka) att det hänt, hur, av vem?

Verktyg: Intrusion Detection Systems (IDSs), digitala signaturer mm.
Exempel: Varning om du loggar in på ny dator!

Kan också se att en attack pågår

Reaction (reaktion) reparera, återskapa, förbättra

Exempel: Prevention - detection - reaction

Prevention vill hindra skador på tillgångar

Använd inte kortnummer öppet online. Kryptera!

Säljaren utför tester (t.ex. leveransadress). Exempel: Roberts filament

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

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!

Åtgärder

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

Låt oss nu gå igenom konkreta åtgärder!

Åtgärder för konfidentialitet

01001001 01000011 01000111

Åtgärder för konfidentialitet

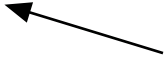
Fysiskt begränsat tillträde

Hinder för stöld av utrustning (larm)

Tillträdeskontroll (inloggning) i datorsystem

Krypterad kommunikation och lagring

Felfria, buggfria program



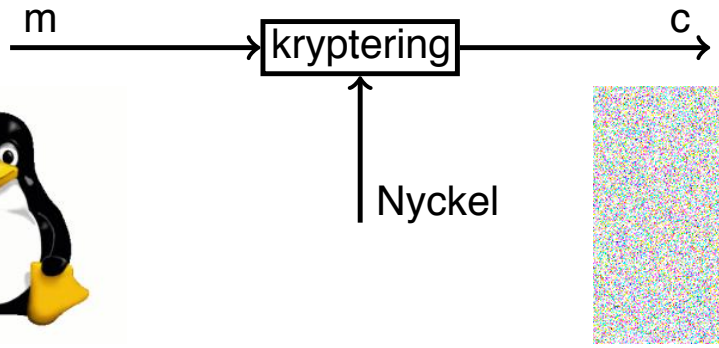
Sagt av någon som inte programmerar?

Åtgärder för konfidentialitet: Kryptering

Ett meddelande krypteras med en nyckel

Meddelandet hålls hemligt för alla som inte har nyckeln

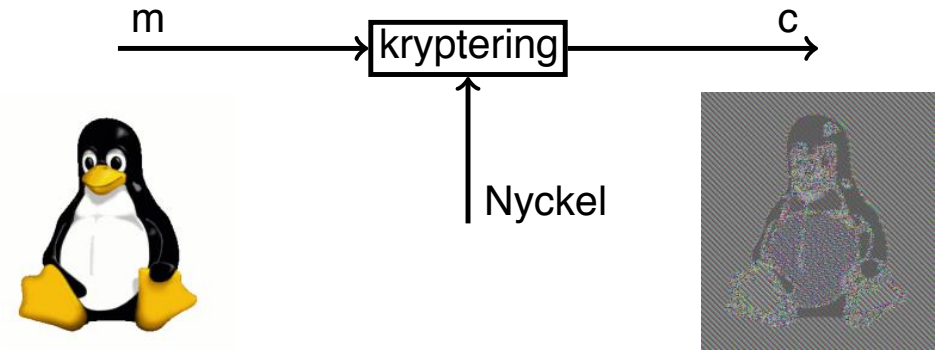
Det finns varianter där alla kan kryptera men bara en kan dekryptera



Åtgärder för konfidentialitet: Kryptering

Bra kryptering döljer all information.

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



Åtgärder för integritet

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

Åtgärder för integritet

Hindra ändringar!

Fysiskt begränsat tillträde

Tillträdeskontroll (inloggning) i datorsystem

Skydd mot ändringar kräver starkare, kryptografiska verktyg

Backuper (även tillgänglighet) - WORM för integritet

Åtgärder för integritet

Verifiera att informationen är korrekt:

Historiskt: Permanent bläck, signering, sigill, stämplar

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

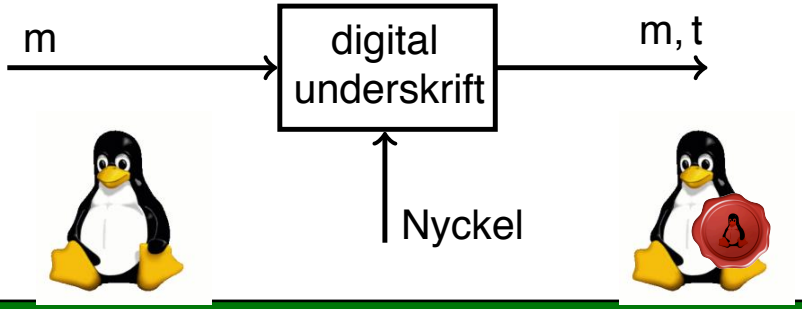


Kryptografiska verktyg för integritet

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



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

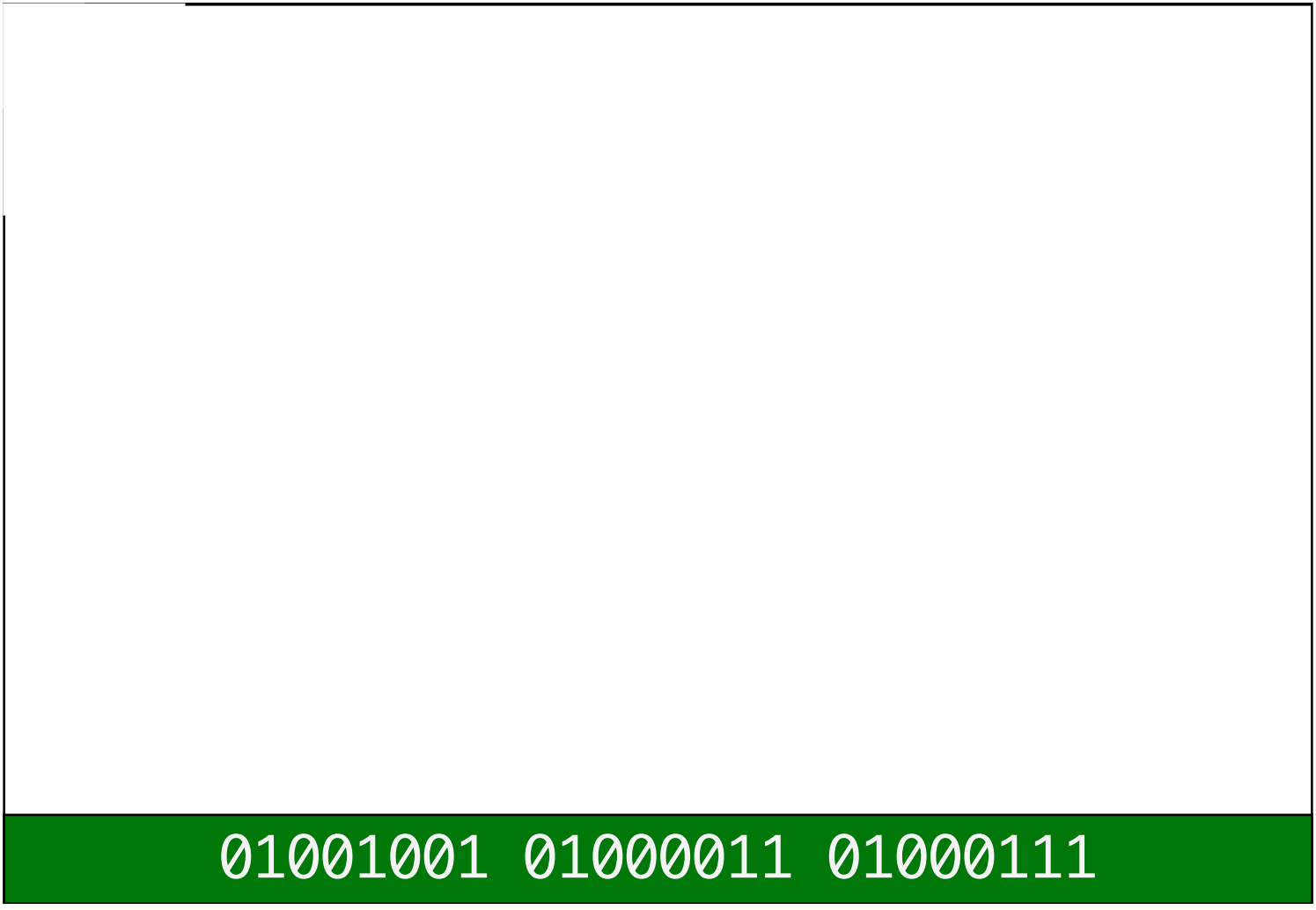
Åtgärder för tillgänglighet

Risker: Dataförlust, förlorad åtkomst

Håll reda på dina lösenord - men inte på en lapp på datorn

Räkna med att data kan förloras

Åtgärd #1:


01001001 01000011 01000111

Dataförlust - Backup svårare än man kan tro

Hindra dataförlust, även från olyckor.

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



Backup svårare än man kan tro

Aktuellt fall (augusti 2023):



ComputerSweden BRANSCH EVENT WHITEPAPERS NYHETSBREV

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.

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

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

01001001 01000011 01000111

Åtgärder för tillgänglighet

Angripare, t.ex. kryptoattacker:

Allt som kan ändras av angriparen kommer att ändras.

Lösning: WORM-backuper

Åtgärder för tillgänglighet

Skydd mot fysiska hot och attacker

- Säker kraftförsörjning
- Brandskydd
- Översvämningsskydd
- Kontrollerad temperatur och luftfuktighet
- Stormtåliga byggnader

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!)

Konfidentialitet och tillgänglighet är knepigt

01001001 01000011 01000111

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

Tips: CIA-analys först, sedan åtgärder!

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?

TACK FÖR IDAG!

01001001 01000011 01000111