IT-osäkerhet

Demo UppLYSning

2004-05-18

Presentatörer

David Lindahl

davli@foi.se

Systemanalys och IT-säkerhet

Forskar inom IT-vapen

Mikael Wedlin

mwe@foi.se

Systemanalys och IT-säkerhet

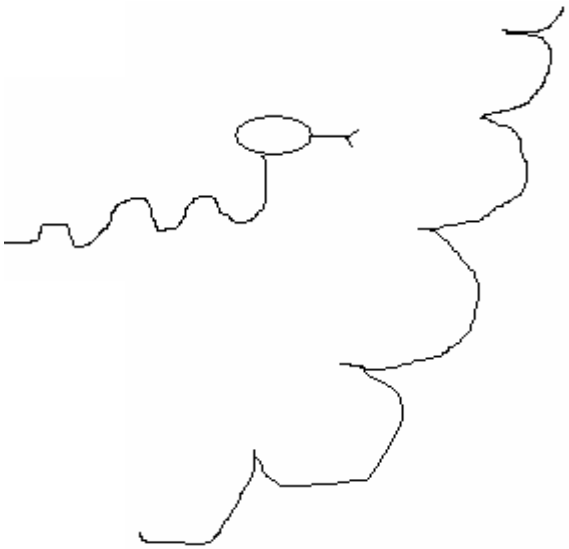
Forskar inom IT-vapen

FOI IT-SÄK

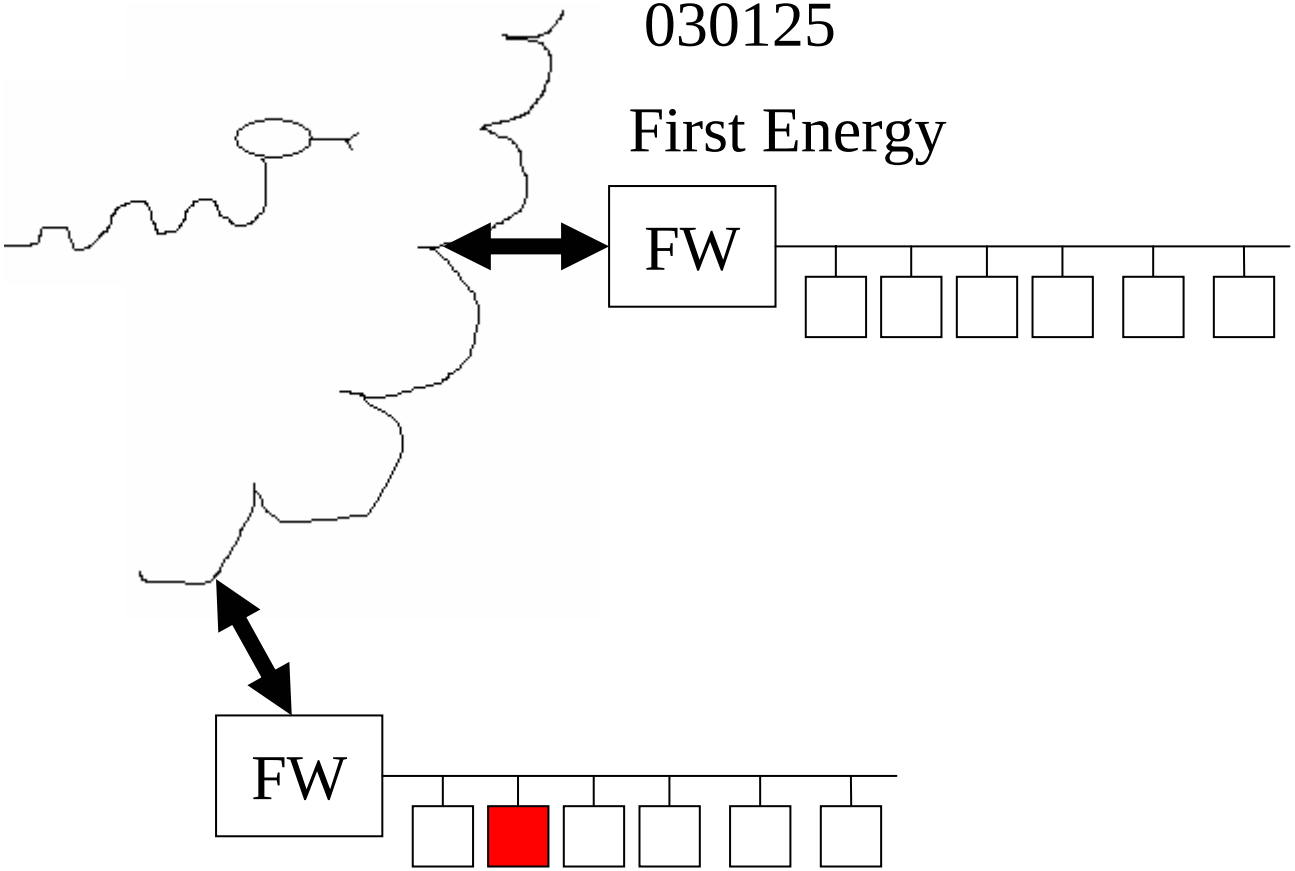
- Tolv personer.
- Ungefär fyra huvudprojekt
- Arbetar åt totalförsvaret och åt företag.
- Vi har expanderat från två personer sedan 1998.
- Nu den största forskningsgruppen inom IT-säk i Sverige

Kort om IT-säkerhet

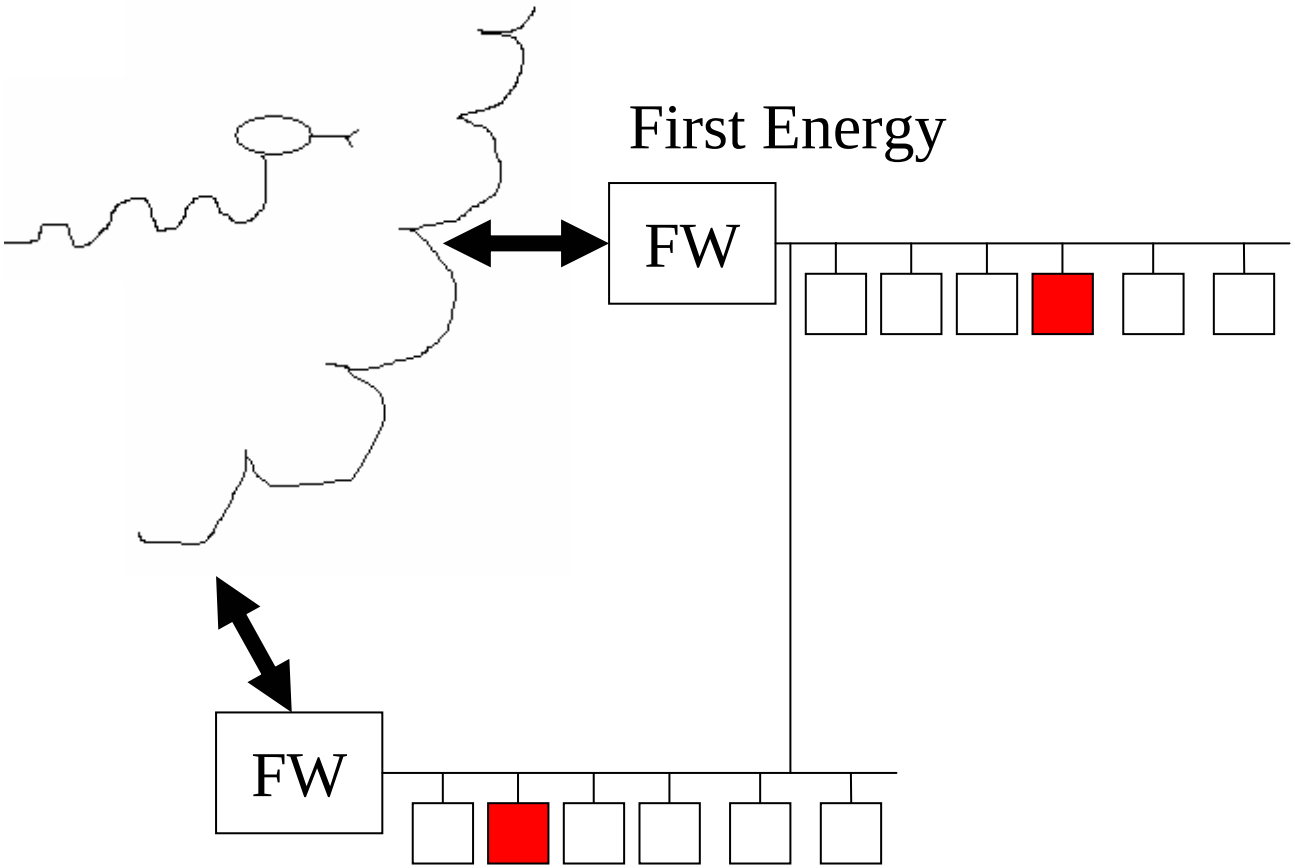
- Det går inte att säkra system i efterhand.
- Användare förstår inte vad som händer i systemen.
- De som designar systemen vet inte under vilka omständigheter de ska användas.
- Kostnad före Nytta före Säkerhet.



Masken Slammer förekommer på Internet. Den sprider sig från dator till dator via nätverk.
Säkerhetsuppdateringar som stoppar masken finns tillgängliga sedan sommaren 2002



Underleverantör



Underleverantör

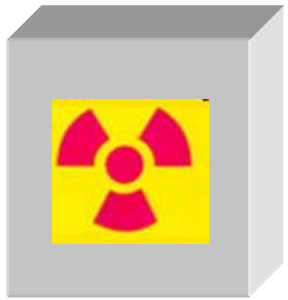
First Energy

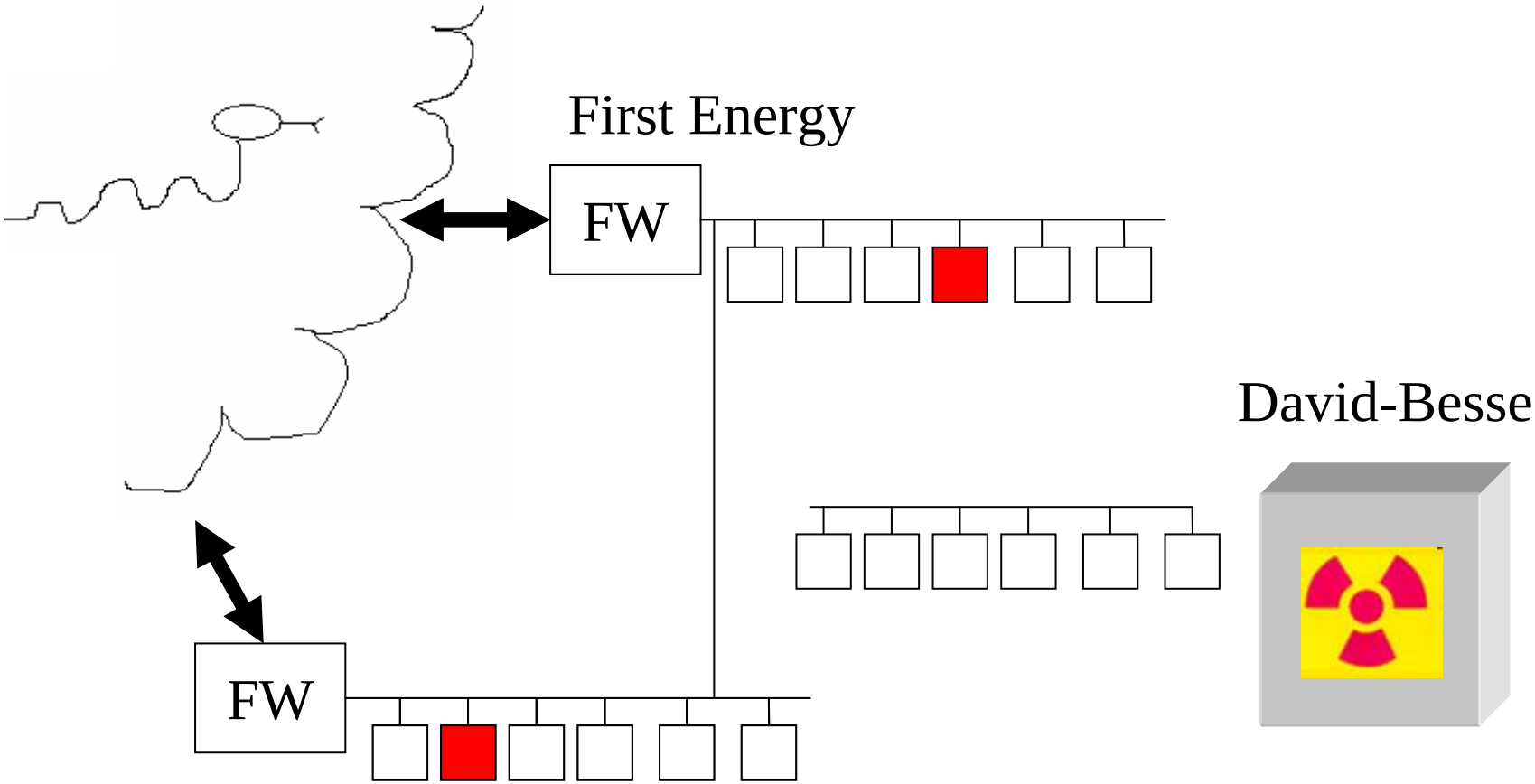
FW

FW

Underleverantör

David-Besse

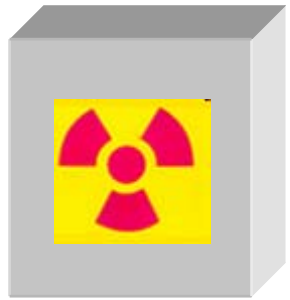



First Energy
FW
David-Besse
FW
Underleverantör

First Energy

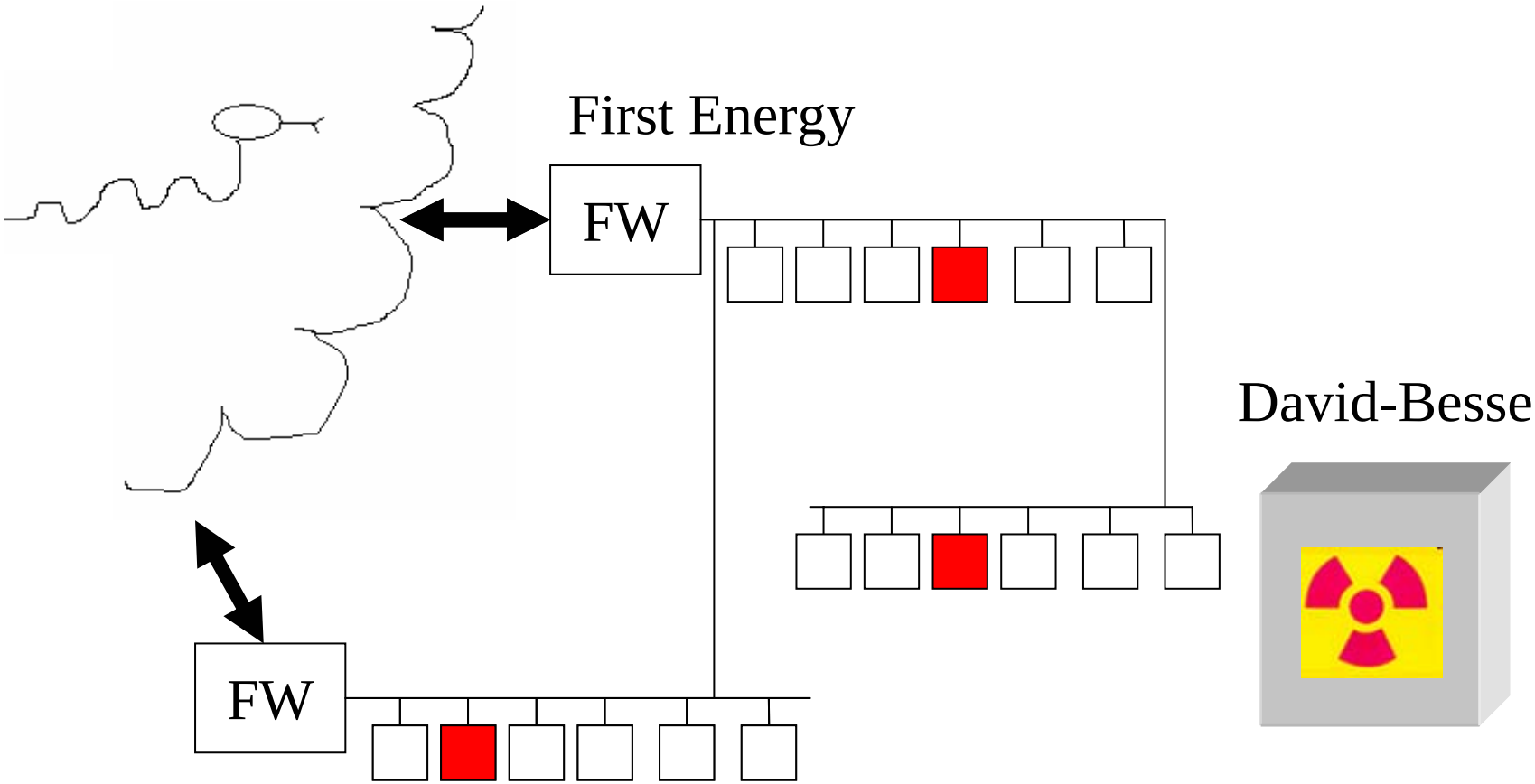
FW

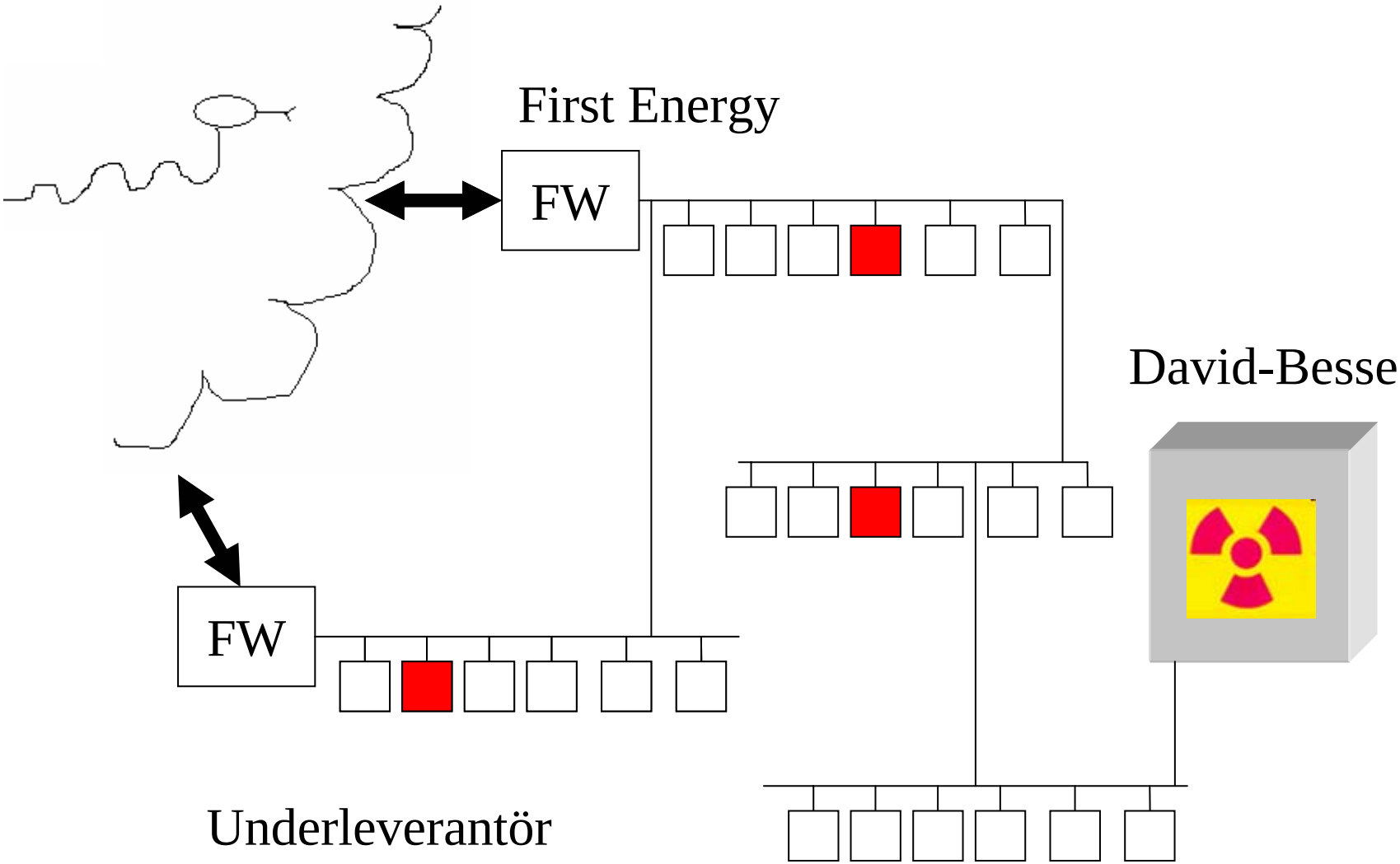
David-Besse

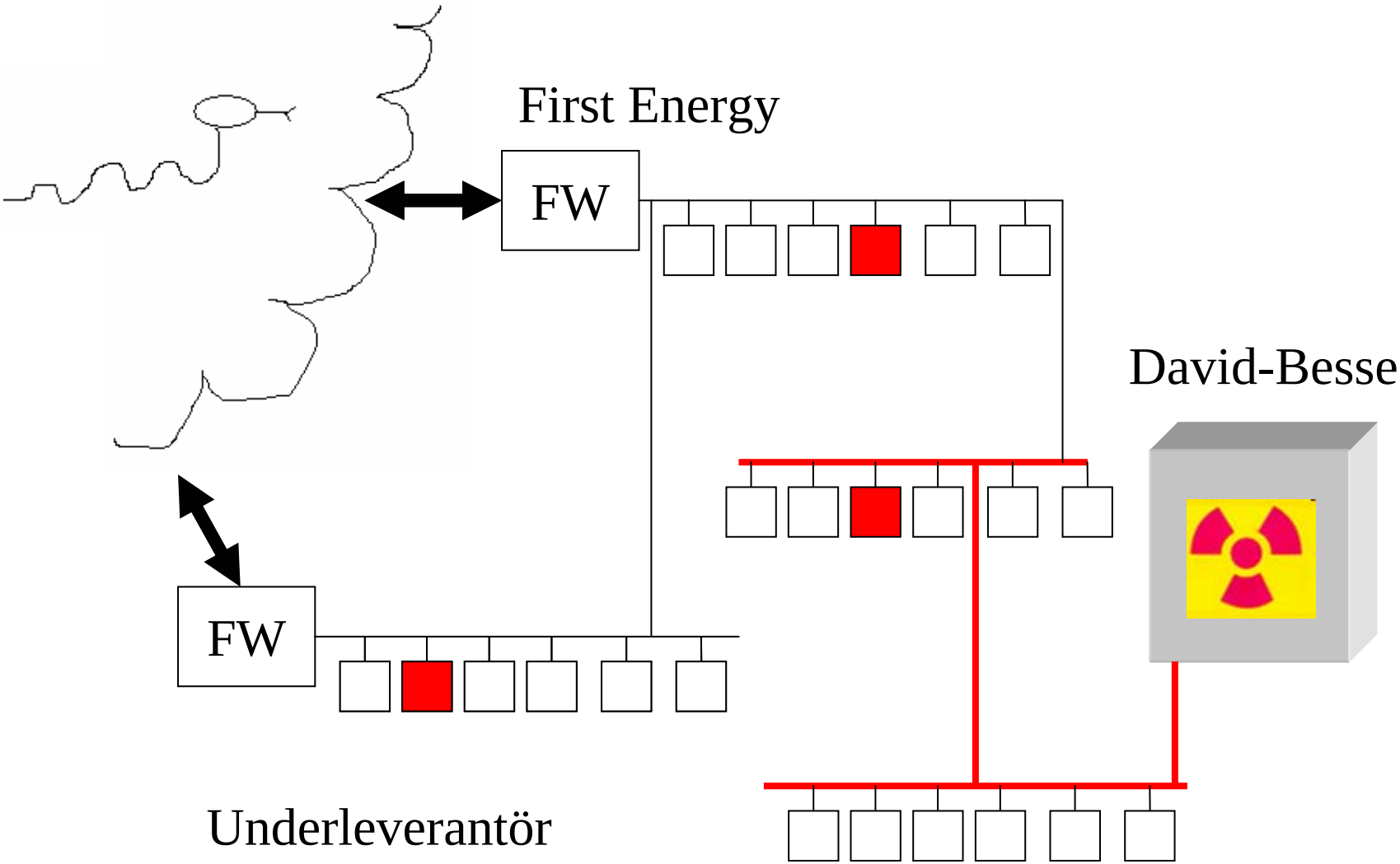


FW

Underleverantör


First Energy
FW
David-Besse
FW
Underleverantör


First Energy
FW
David-Besse
FW
Underleverantör


First Energy
FW
David-Besse
FW
Underleverantör

David-Besse Nuclear Power Plant 030125

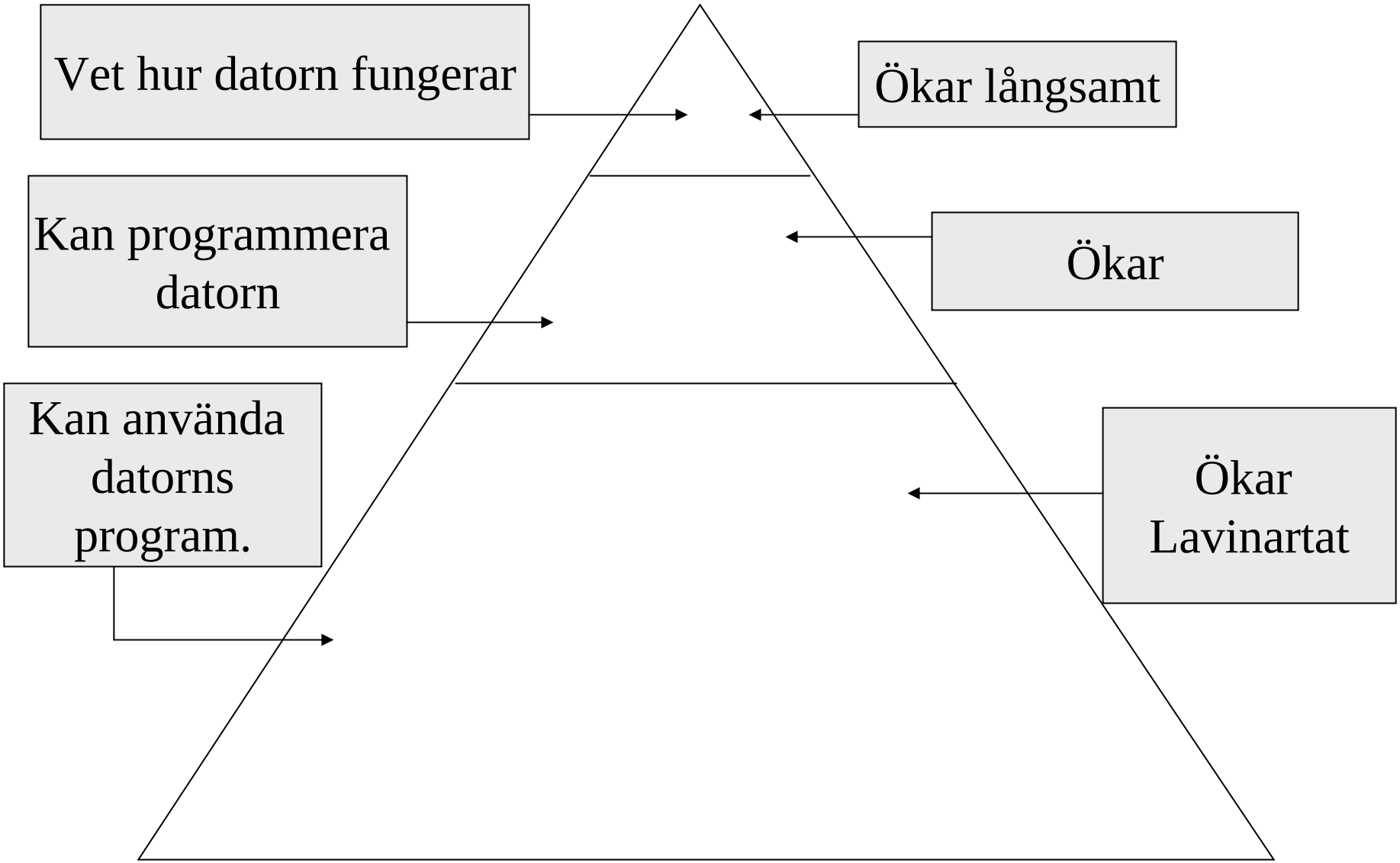
- Slammer-masken kom in i en underleverantörs system.
- Underleverantören hade en koppling förbi brandväggen in i First Energys kontorsdatornät.
- Kontorsdatornätet hade en koppling in i kärnkraftverkets datornätverk för att hämta data om drift.

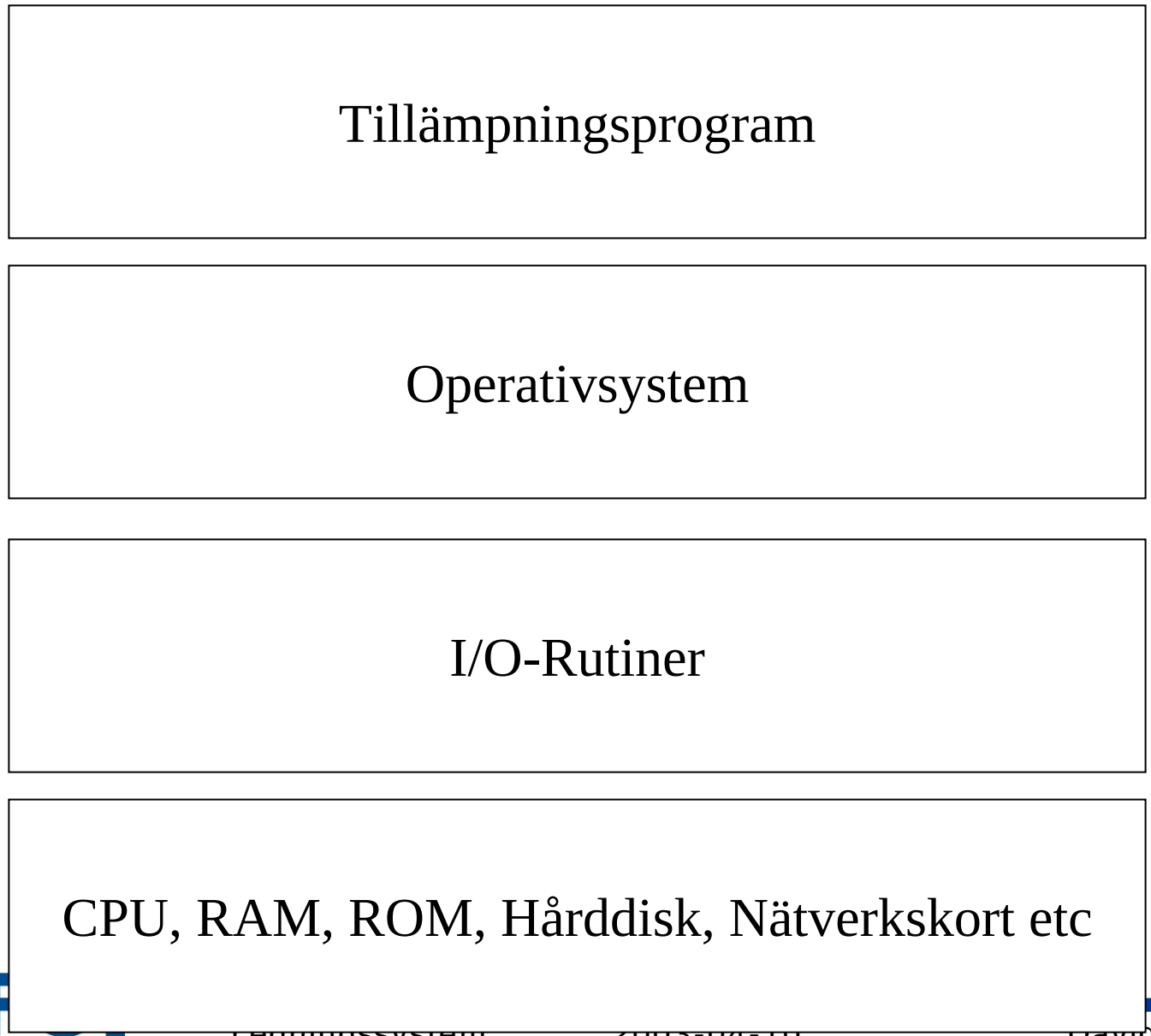
David-Besse Nuclear Power Plant 030125

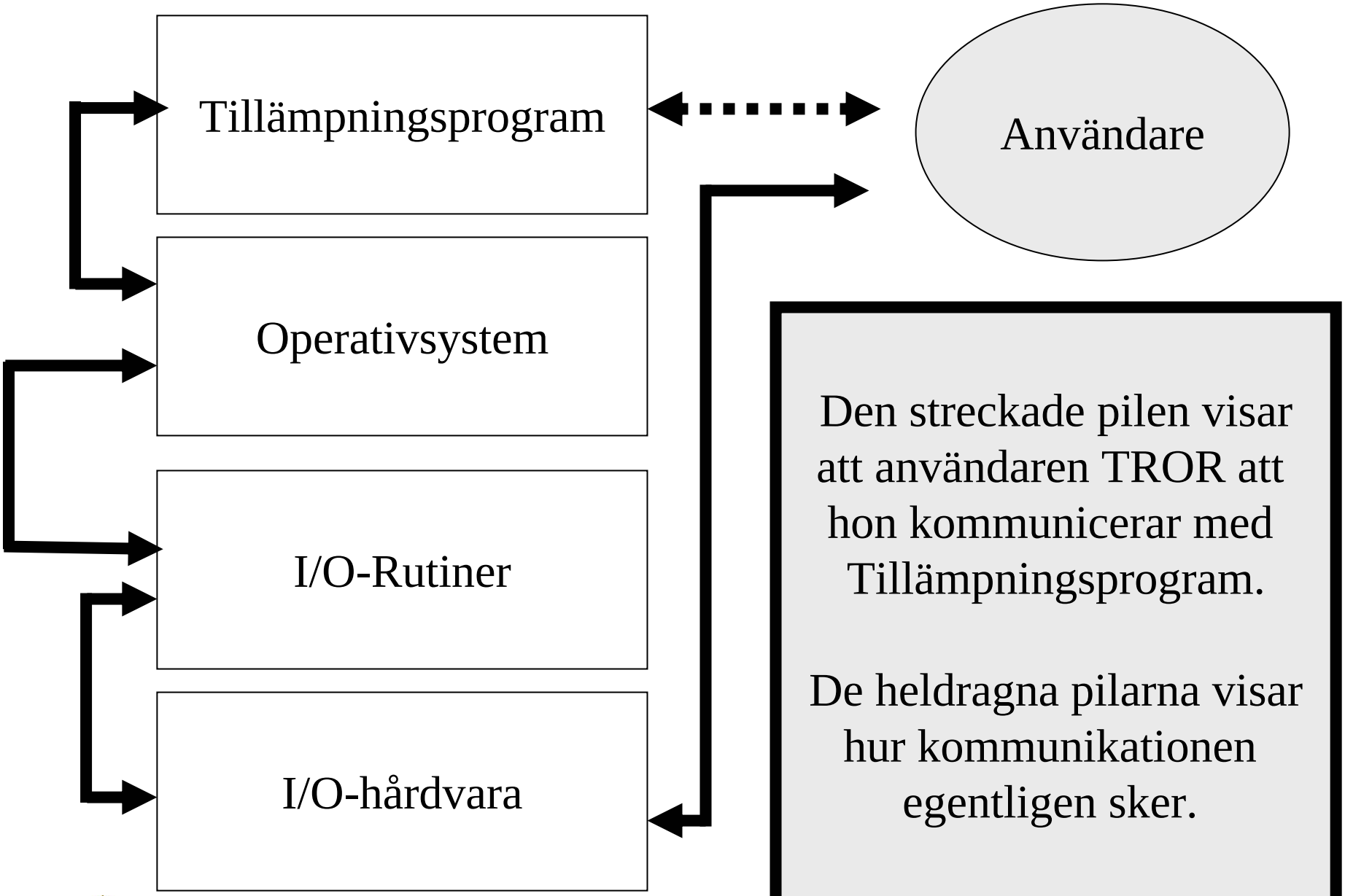
- Interna datorer var inte uppdaterade mot Slammer.
- Brandväggar separerade inte alla vägar mellan driftdatornät och administrationsdatornät.
- Det digitala övervakningssystemet gick ner. Det analoga reservsystemet fungerade fortfarande.
- Det enda skälet till att man inte nödstoppade var att verket var nere för underhåll.

David-Besse Nuclear Power Plant 030125

Vems var felet att detta hände?


Vet hur datorn fungerar
Ökar långsamt
Kan programmera datorn
Ökar
Kan använda datorns program.
Ökar Lavinartat


Tillämpningsprogram
Operativsystem
I/O-Rutiner
CPU, RAM, ROM, Hårddisk, Nätverkskort etc


Tillämpningsprogram
Användare
Operativsystem
I/O-Rutiner
I/O-hårdvara
Den streckade pilen visar att användaren TROR att hon kommunicerar med Tillämpningsprogram.
De heldragna pilarna visar hur kommunikationen egentligen sker.

IT-vapen

- Informationskrigföring
- Datorkrigföring
- Nätverksoperationer
- IT-vapen

Scenaria

- Vi har gjort tre olika scenaria
- De exemplifierar alternativa situationer där datorkrigföring förekommer.

Scenariafrågor.

- Är detta teoretiskt/tekniskt genomförbart?
- Är detta praktiskt genomförbart?
- Möjligt utfall av operation?
- Troligt utfall av operation?
- Resursinvestering?
- Aktörer med sådana resurser?

- Alternativa metoder för samma utfall?
- Motiv som presenteras i scenario?
- Rimlighet, Alternativa motiv?
- Vilka åtgärder skulle hindrat angriparen?
- Finns det någon koppling till det civila samhället?

Orientering

- UND:s nya roller.
- SIGINT (Echelon)
  - RÖS (NIR, skrivare, skärmar, 802.11b)
  - Chipping
- Kinas syn på IT-krig
- Rysslands syn på IT-krig (COPM)
- USA:s syn på IT-krig (Crimson Sunrise)

Målen för IT-krig

- Militära Ledningssystem
  - Luftförsvarssystem
  - Lägesbildsystem
  - Kommunikationssystem
- Civila Ledningssystem
- Militära Logistiksystem
- Civila Logistiksystem
- Massmedier
- Syndabockar

Problem med IT-krig ur en militär synvinkel

- Svårförutsägbar verkan
- Kollateralskadorna blir enorma
- Måldifferentiering
- Målidentifiering
- Dagens vapen är lätt detekterbara
- Relativt enkla medel hindrar dem när de väl identifierats
- Juridiskt minfält

Moderna Tillämpningsprogram

Exempel på Säkerhetsbrister

Faran med "features"

- Ett problem som har blivit allt mer accentuerat de senaste åren är att antalet finesser ("features") i programmen har blivit allt fler. (Så kallad Feature Creeping)
- Detta är ett säkerhetsproblem på grund av att kombinationer av finesser producerar svårförutsägbara resultat.

Sammanfattning av 1917 års bibel på 20 meningar

13,1. Upp. 2,9. Upp. 6. Och HERREN, din Gud. 20,12. Upp. 4,24. 14,15. Upp. 6. Du allena är HERREN. >Upp. 2,6. Upp. >Upp. 2,6. Upp. 7,34. 16,9. 33,11. Upp. 51,7. Upp. 51,6, 45. Upp. 50,8. Upp. 46,11. Upp. >Upp. >Upp. 3,24. Upp. 10,9. Upp. 15. Och du.

Ett mer seriöst exempel

- I Word 97 kan man under Tools/Options/Save kryssa i valet "Allow fast saves".
- Det får mycket intressanta effekter ur säkerhetssynpunkt.

"Allow Fast Save"

- Om detta val har aktiverats kommer information som raderas ur dokumentet inte att försvinna utan bara att markeras som tillfälligt dold.
- Det innebär att raderad information lätt kan hittas till exempel genom att öppna dokumentet i en editor.

Räddning

- Slå av Fast Save.
- Har dokument tidigare sparats med Fast save kan de fixas:
  - Välj "Spara som" och spara dokumentet under ett NYTT NAMN
  - Att använda "Spara Som" med samma namn hjälper inte.

Easter Eggs

Skämt eller sabotage?

Påskägg

- Programmerare tenderar att gömma roliga skämt i program som man kan få fram genom vissa udda tangentkombinationer.
- Exempel på sådana är flygsimulatorn i Excel 97 och flipperspelet i Word 97

Säkerhet

- Varför tar jag upp påskägg i en föreläsning om säkerhet?

Påskägg

- Testningen av datorprogram är i dag så dålig att programmerare i praktiken kan lägga till vfsh.
- Det finns i dag inga verktyg för att analysera program efter leverans
- Programvarubranschen har ett ”mindre bra” kvalitetstänkande

Sårbarheter

- Ett påskägg är lagringsutrymme som kan användas för att föra in vapen.
- Eftersom de ofta är stora kan checksummeutfyllnad få plats runt vapnet.
- Kända påskägg i vitt spridda program blir då högvärda mål.

Snabbfix

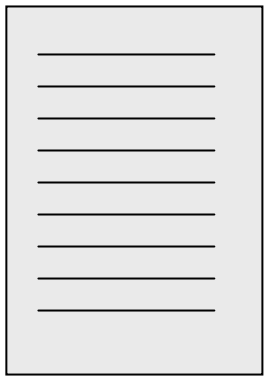
- Saknas.
- Ett alternativ skulle kunna vara att systematiskt rensa ut alla kända påskägg ur sina program men det är en lösning som verkar mycket svår att genomföra i praktiken.

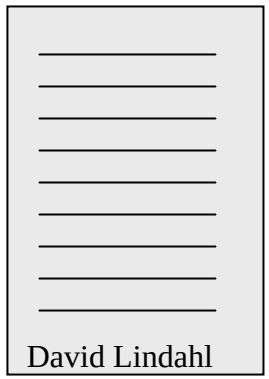
Missbruk av digitala signaturer

Digitala signaturer inledning

- Digitala signaturer är datorvärldens versioner av underskrifter.
- Alla svenskar ska få en sådan för att kunna identifiera sig via datorn.
- Man kan redan deklarera m h a signaturer. Så småningom ska man kunna interagera med alla myndigheter på så sätt.

Digitala signaturer





1001010
0010101
0111010
1000101
0111010

1001010
0010101
0111010
1000101
0111010
1101010

Meddelande Signerat

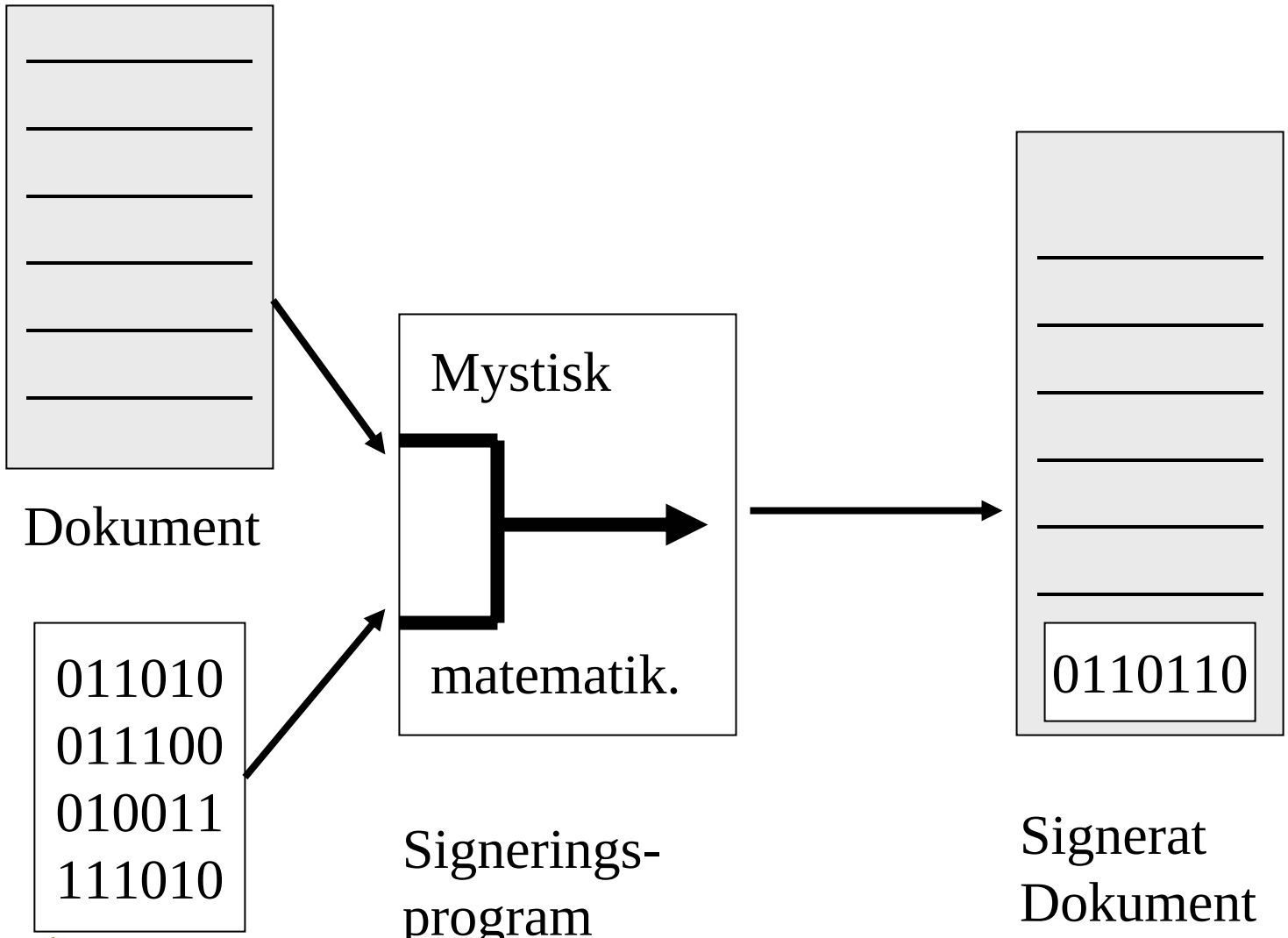
Fil Signerad Fil

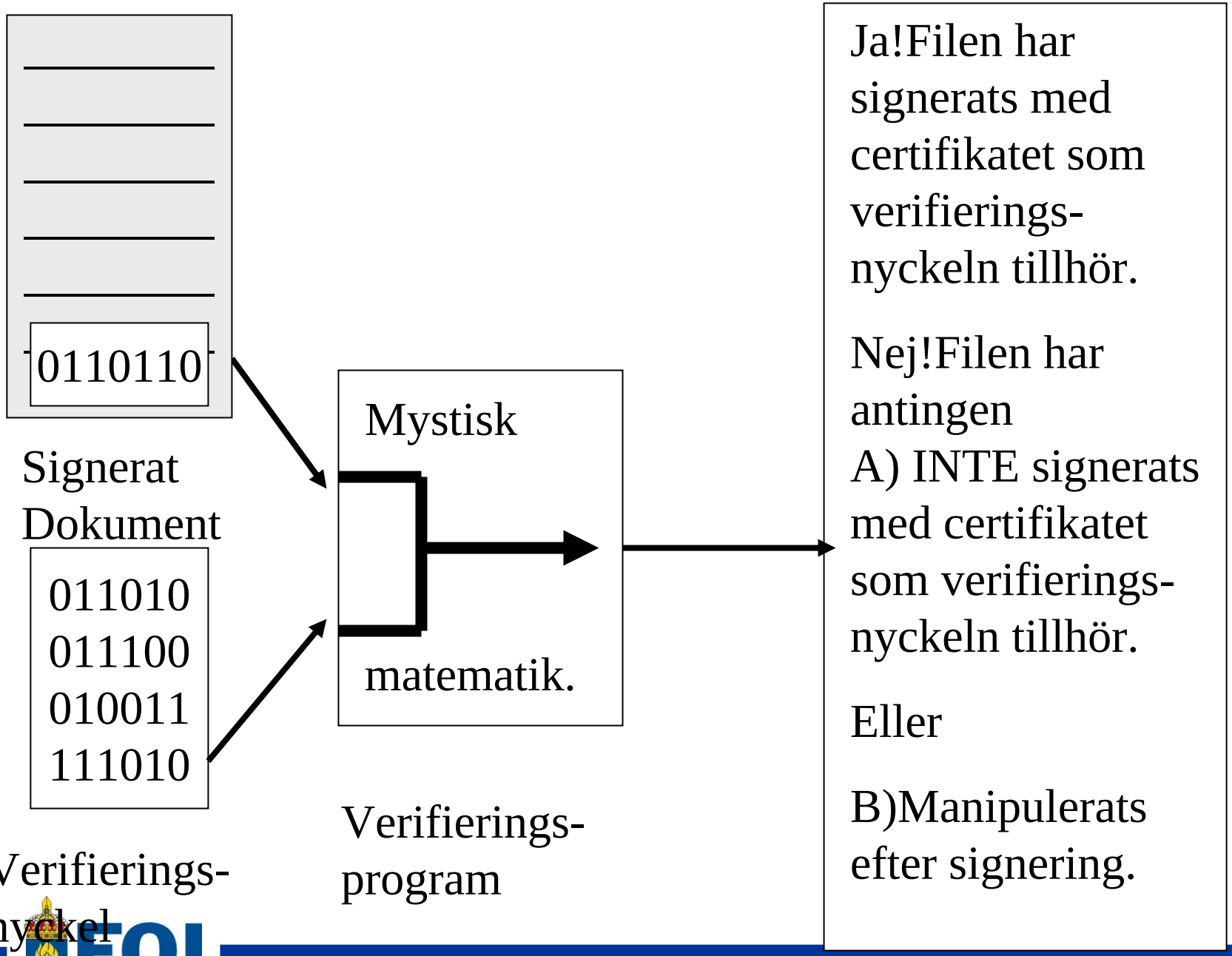
Digitala certifikat forts

- Ett certifikat är ett intyg i stil med ett ID-kort.
- Till ett certifikat hör två nycklar i stil med de som används för kryptering.
- Den ena nyckeln används för att certifiera, eller skriva under, filer.
- Den andra nyckeln används för att verifiera att rätt nyckel använts för att skapa underskriften.

Digitala certifikat forts

- Verifieringsnyckeln och information om vems certifikat den hör ihop med kan (och ska) spridas fritt.
- Normalt lämnas det ut av samma organisation som delat ut originalcertifikatet.


Dokument
011010
011100
010011
111010
Mystisk
matematik.
0110110
Signerings-
program
Signerat
Dokument


0110110
Signerat Dokument
011010
011100
010011
111010
Verifierings-nyckel
Mystisk
matematik.
Verifierings-program
Ja!Filen har signerats med certifikatet som verifierings-nyckeln tillhör.
Nej!Filen har antingen
A) INTE signerats med certifikatet som verifierings-nyckeln tillhör.
Eller
B)Manipulerats efter signering.

Certifikatdemo

- Ett av problemen med certifikat är att få alla att förstå vad som egentligen händer när ett certifikat används. Det man signerar är den digitala representationen av en fil. Inte det ett program visar på skärmen.
- Om någon slarvar med sin signeringsnyckel kan andra underteckna bindande avtal el dyl I dennes namn.

Förändrade Virus

- En dator med W2000 har köpts in.
- För att säkra den mot virus installerar vi Norton Antivirus CD på den.
- Därefter ansluter vi den till ett datornätverk.

Förändrade virus

- De datorvirus som finns tillgängliga på Internet kan lätt ändras så att de inte längre fångas upp av Antivirusprogram
- Vi har tagit ett virus som heter Homepage och manipulerat det.

Förändrade virus forts.

- Homepage leverades kodad i ett Visual Basic Script.
- Kodningen var att programkoden förskjutits två steg i ASCII-tabellen och att vissa tecken specifikt hade ersatts med andra tecken.
- Vid körning avkodades viruset och kördes.

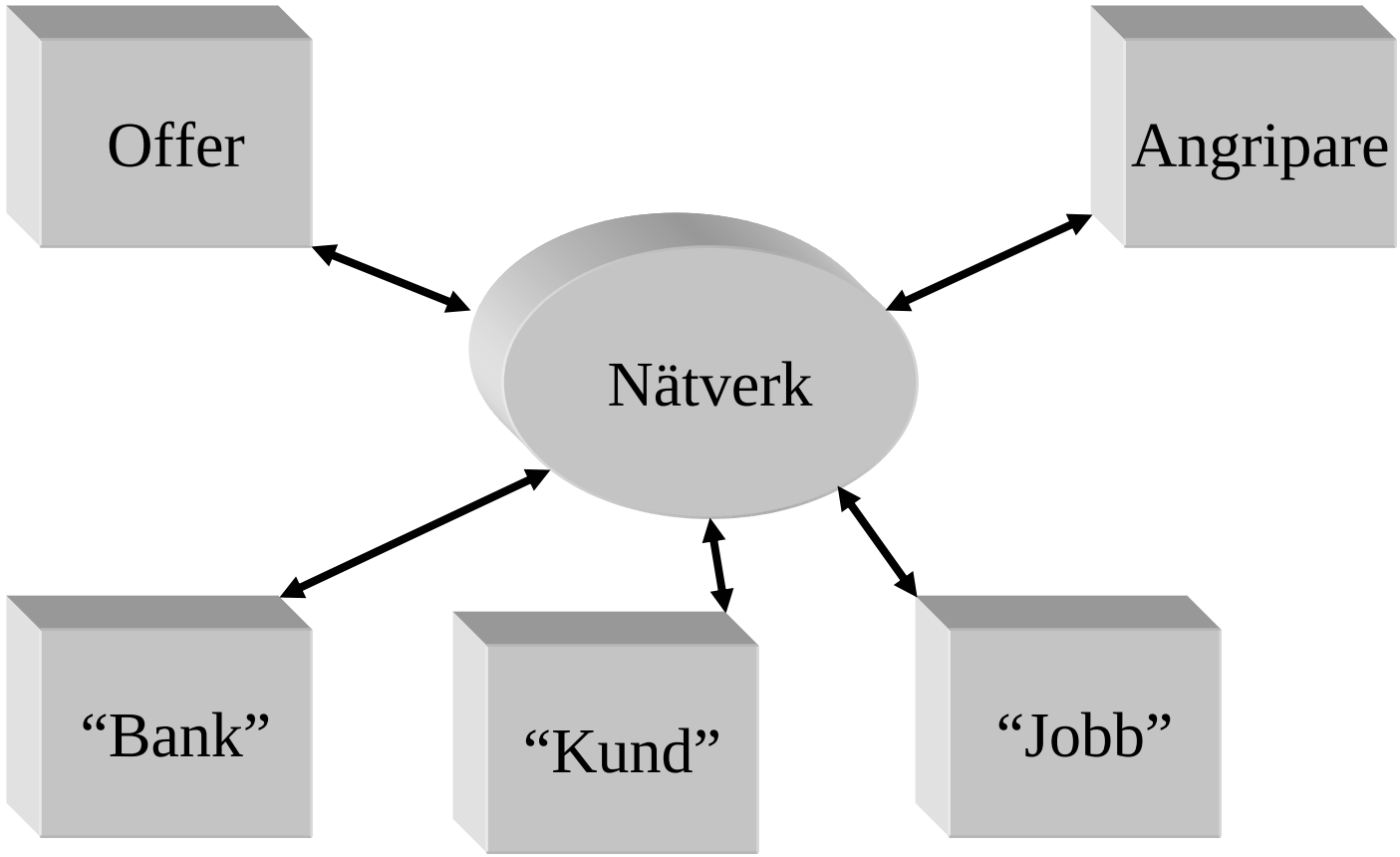
Förändrade virus Demo

- Vi tog originalviruset som Norton Antivirus stoppar.
- Därefter ändrade vi kodningen så att vi försköt koden tre steg i stället för två, samt
- Att blanksteg kodades annorlunda.

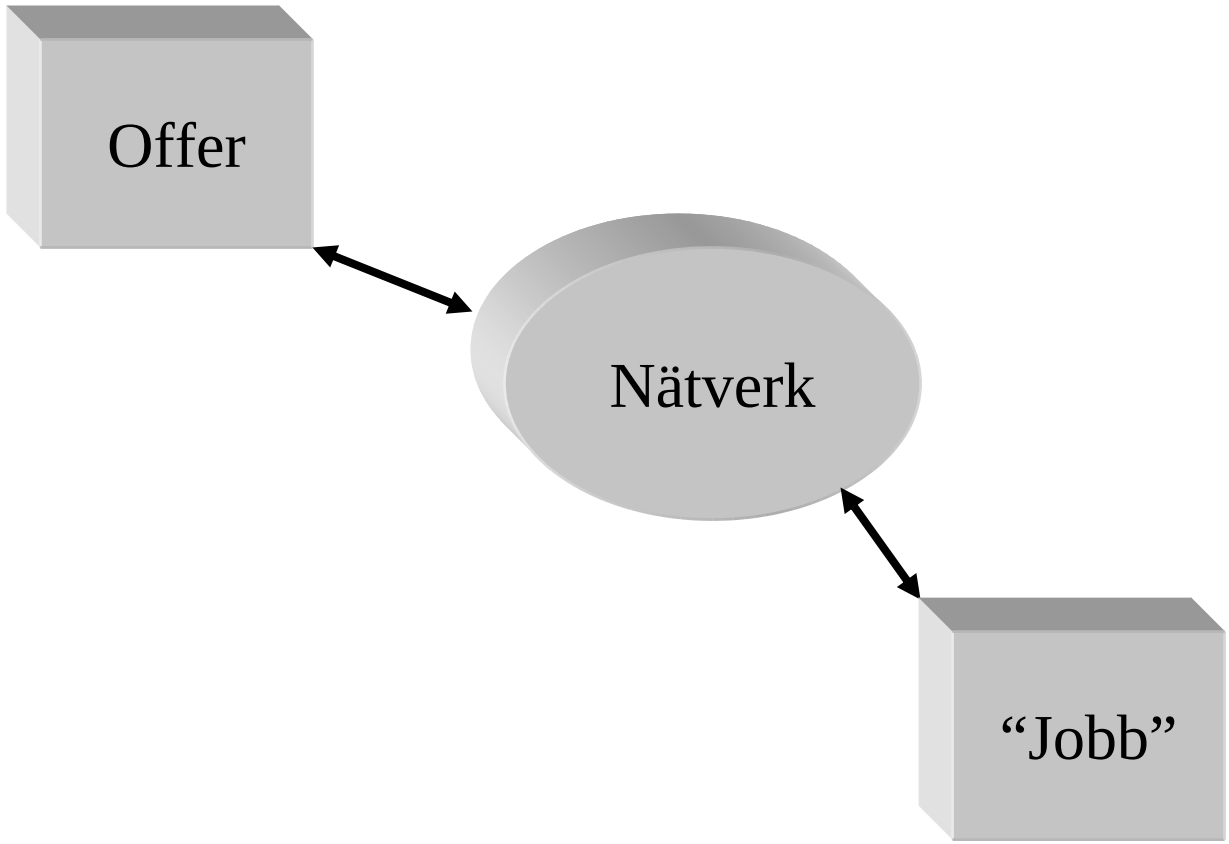
Slutsatser

- Vapen som inte hittas av antivirusprogram är lätta att tillverka även för amatörer.
- Antivirusprogram måste hållas ständigt uppdaterade.
- Ett värdefullt system måste ha användare som beter sig riskmedvetet. Det innebär utbildade användare.

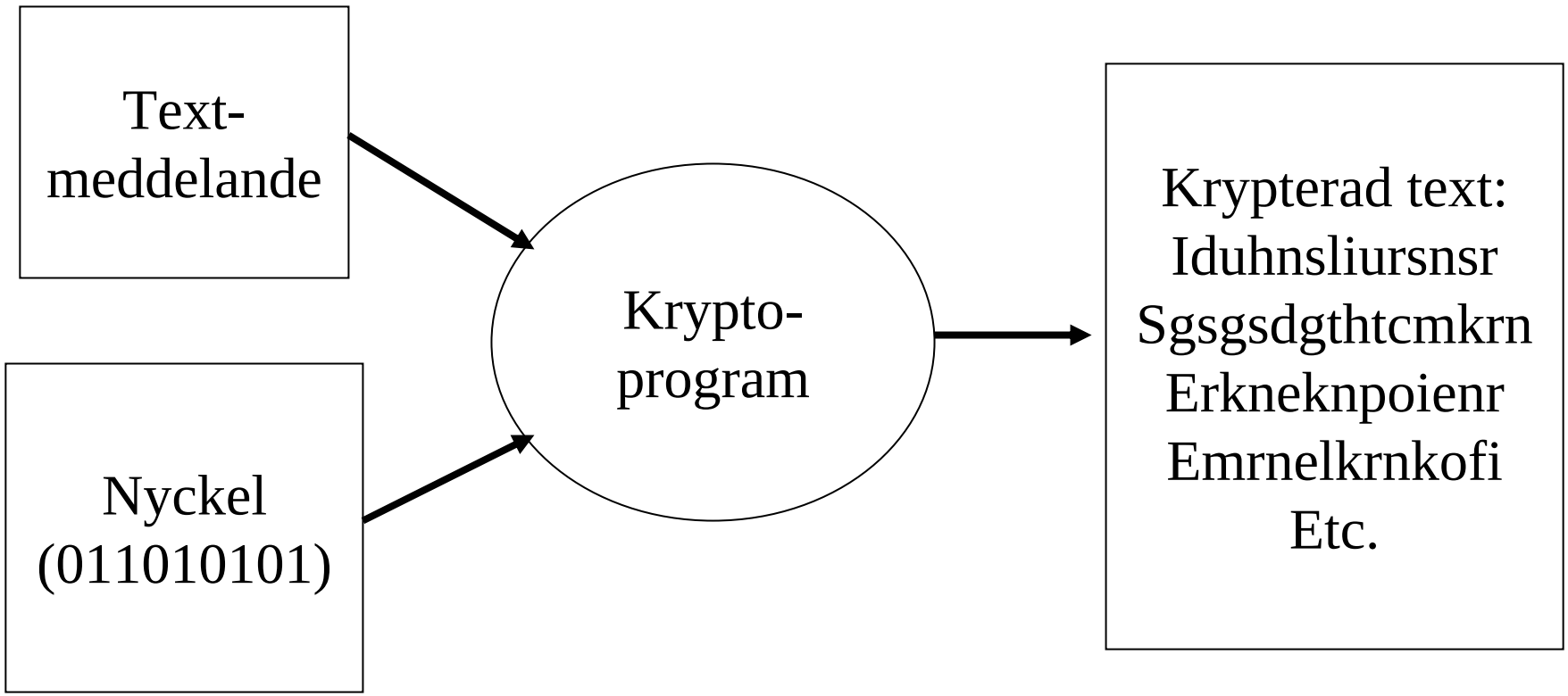
Demonstrationssystemet



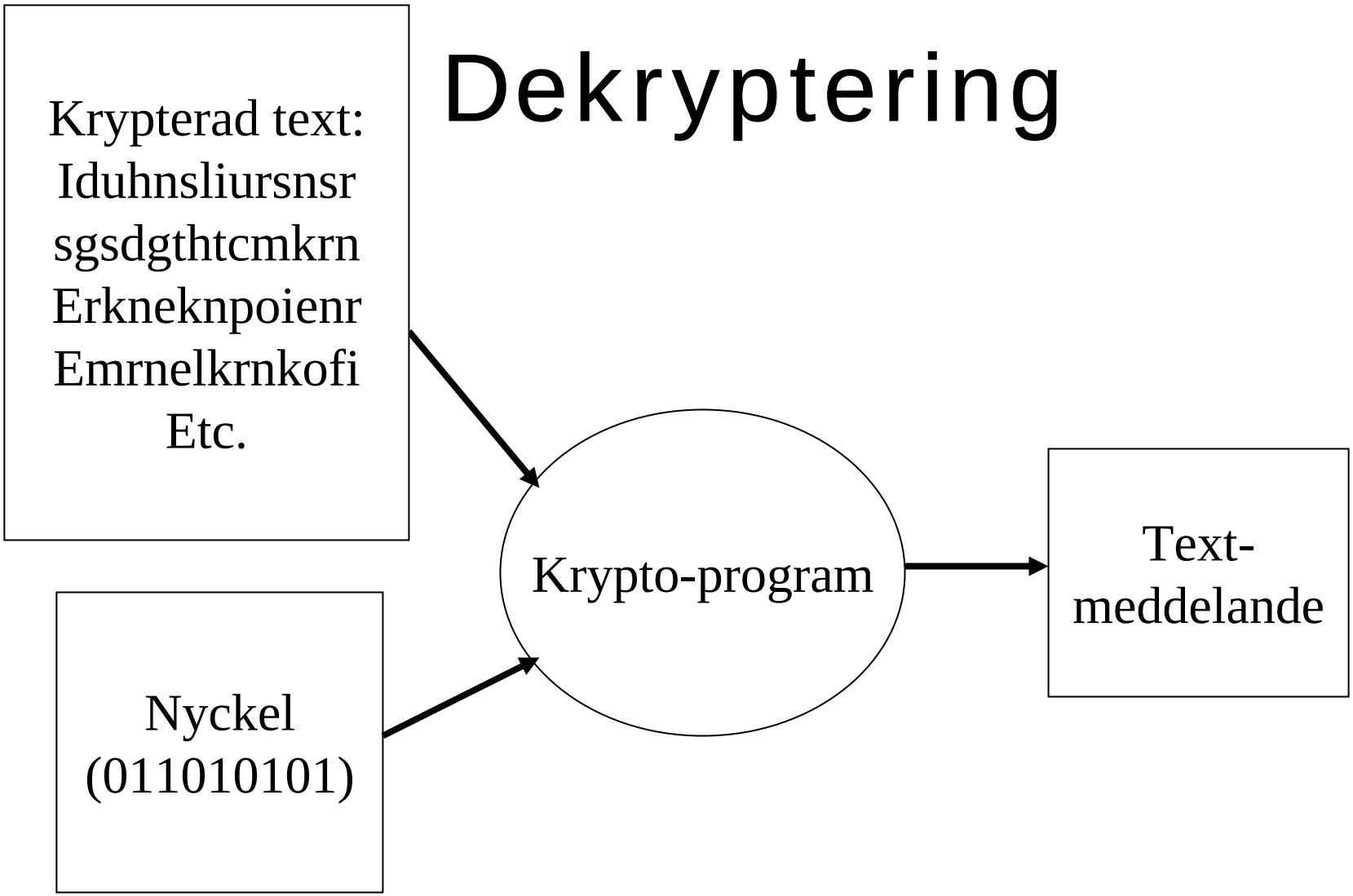
Arbeta mot annan dator: SSH



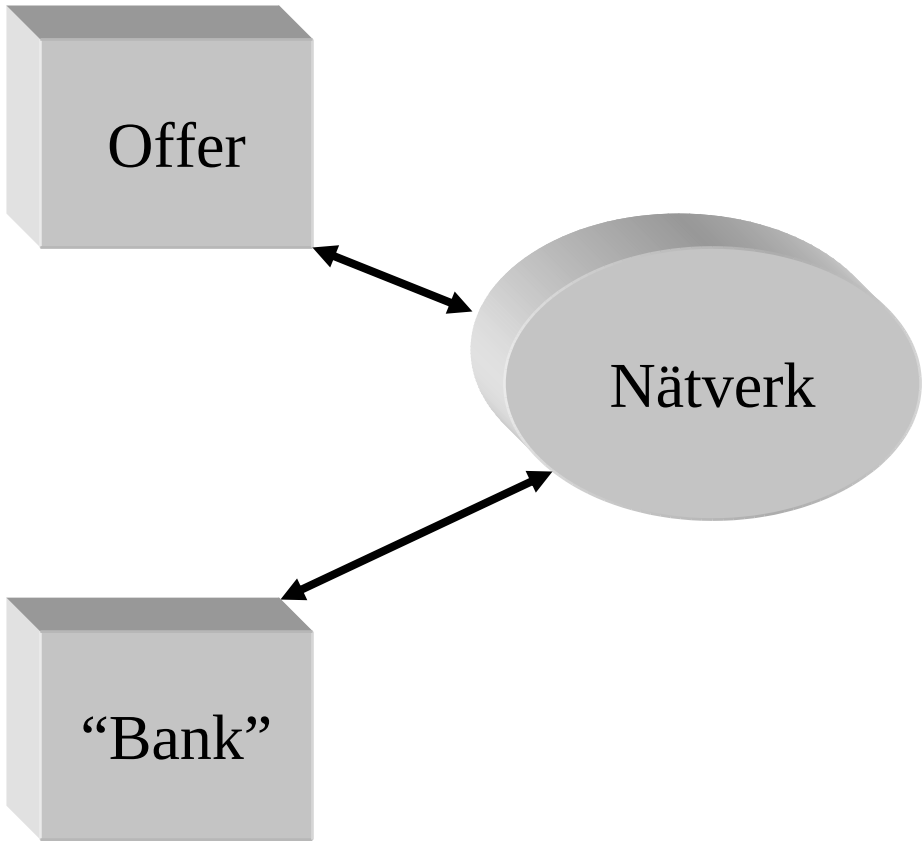
Kryptering


Text-
meddelande
Nyckel
(011010101)
Krypto-
program
Krypterad text:
Iduhnsliursnsr
Sgsgsdgthtcmkrn
Erkneknpoienr
Emrnelkrnkofi
Etc.

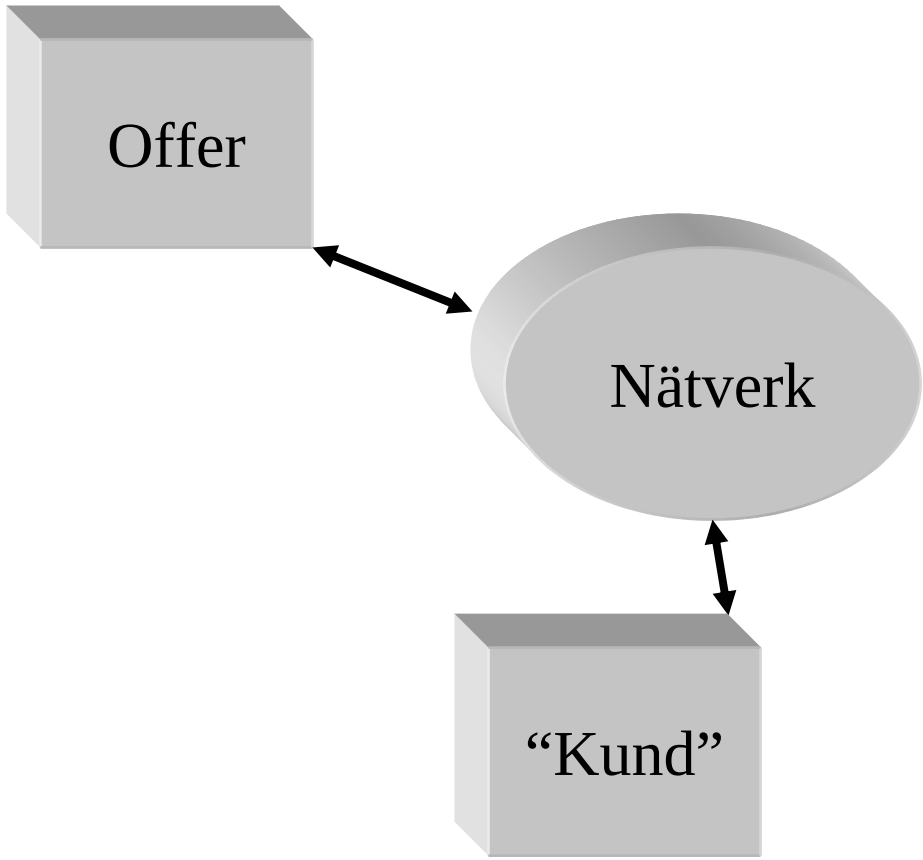
Dekryptering



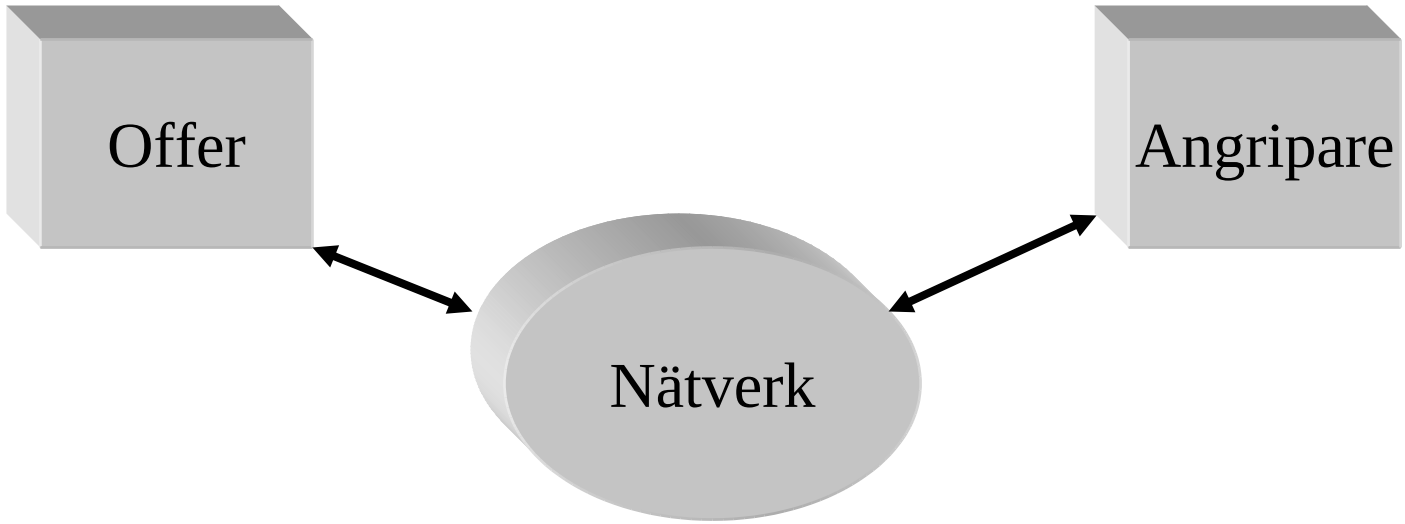
Bankärenden



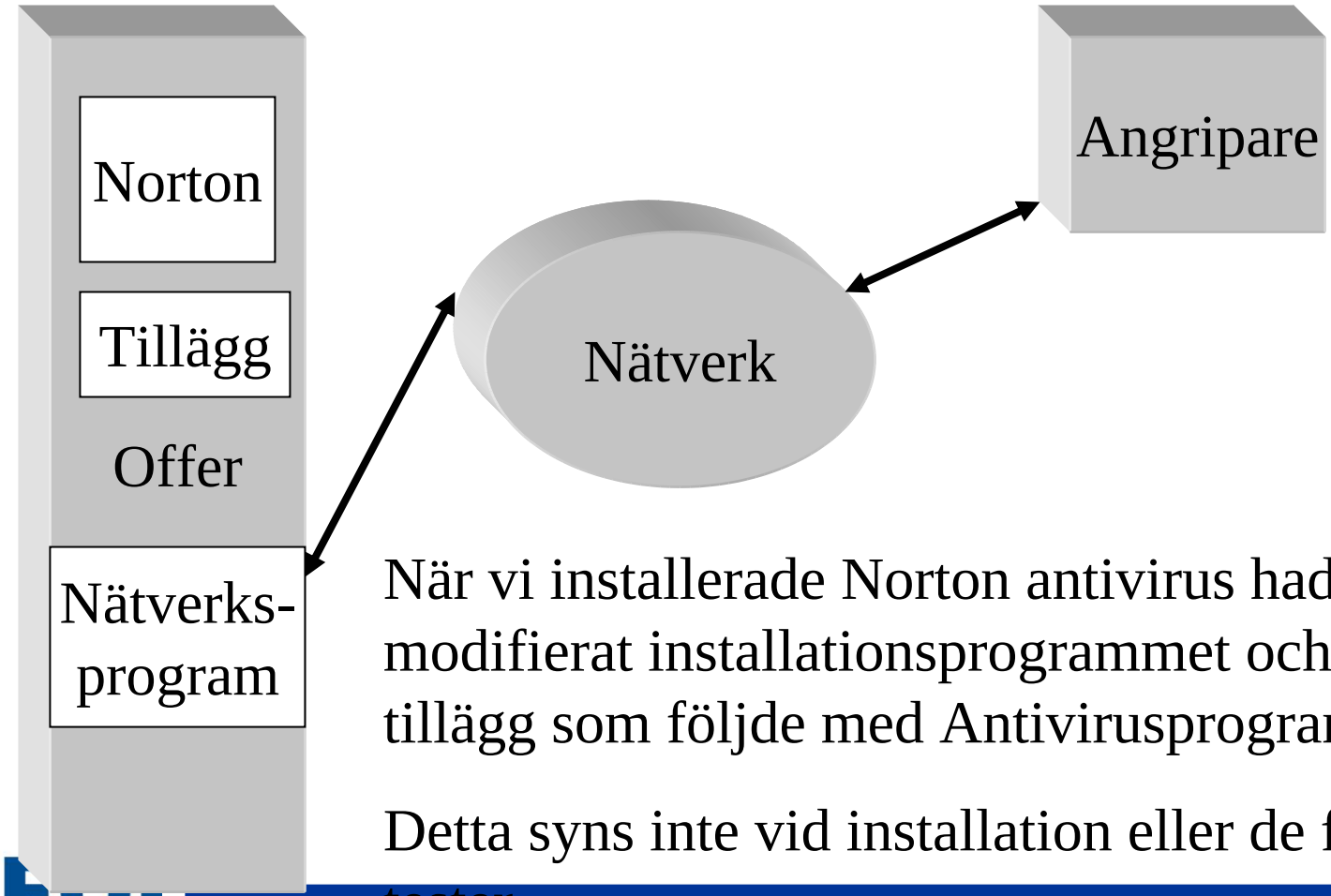
Skriva kundbrev.



Angrepp



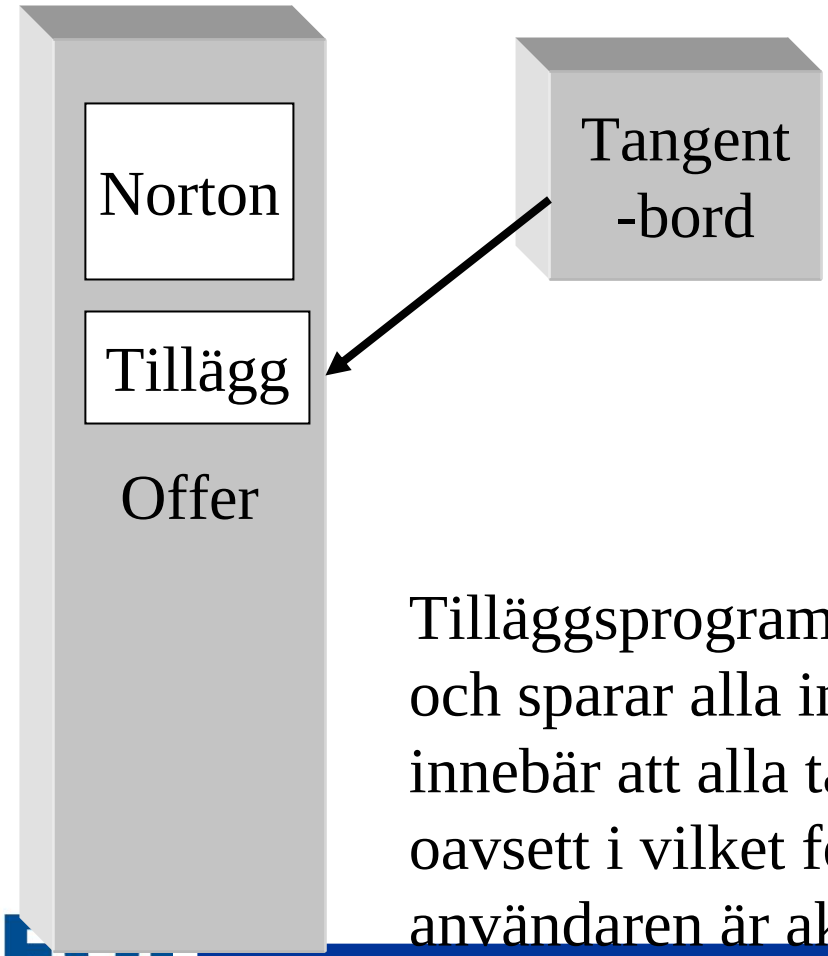
Detaljer



När vi installerade Norton antivirus hade vi modifierat installationsprogrammet och gjort ett tillägg som följde med Antivirusprogrammet.

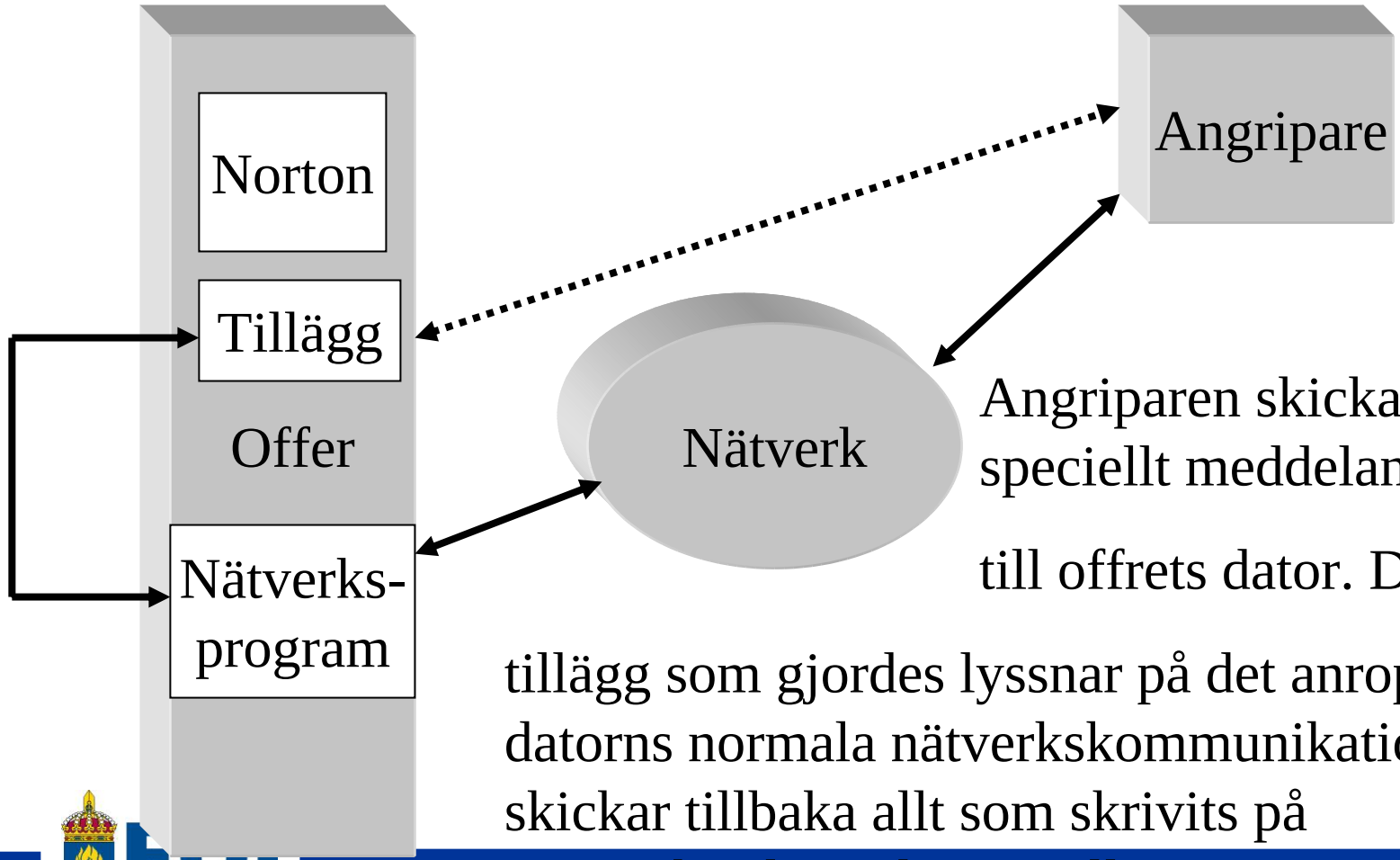
Detta syns inte vid installation eller de flesta tester.

Detaljer, forts



Tilläggsprogrammet lyssnar på tangentbordet och sparar alla inkommande signaler. Det innebär att alla tangentnertryckningar sparas oavsett i vilket fönster eller program användaren är aktiv.

Detaljer forts



Angriparen skickar ett speciellt meddelande till offrets dator. Det tillägg som gjordes lyssnar på det anropet via datorns normala nätverkskommunikation och skickar tillbaka allt som skrivits på tangentbordet sedan installationen.

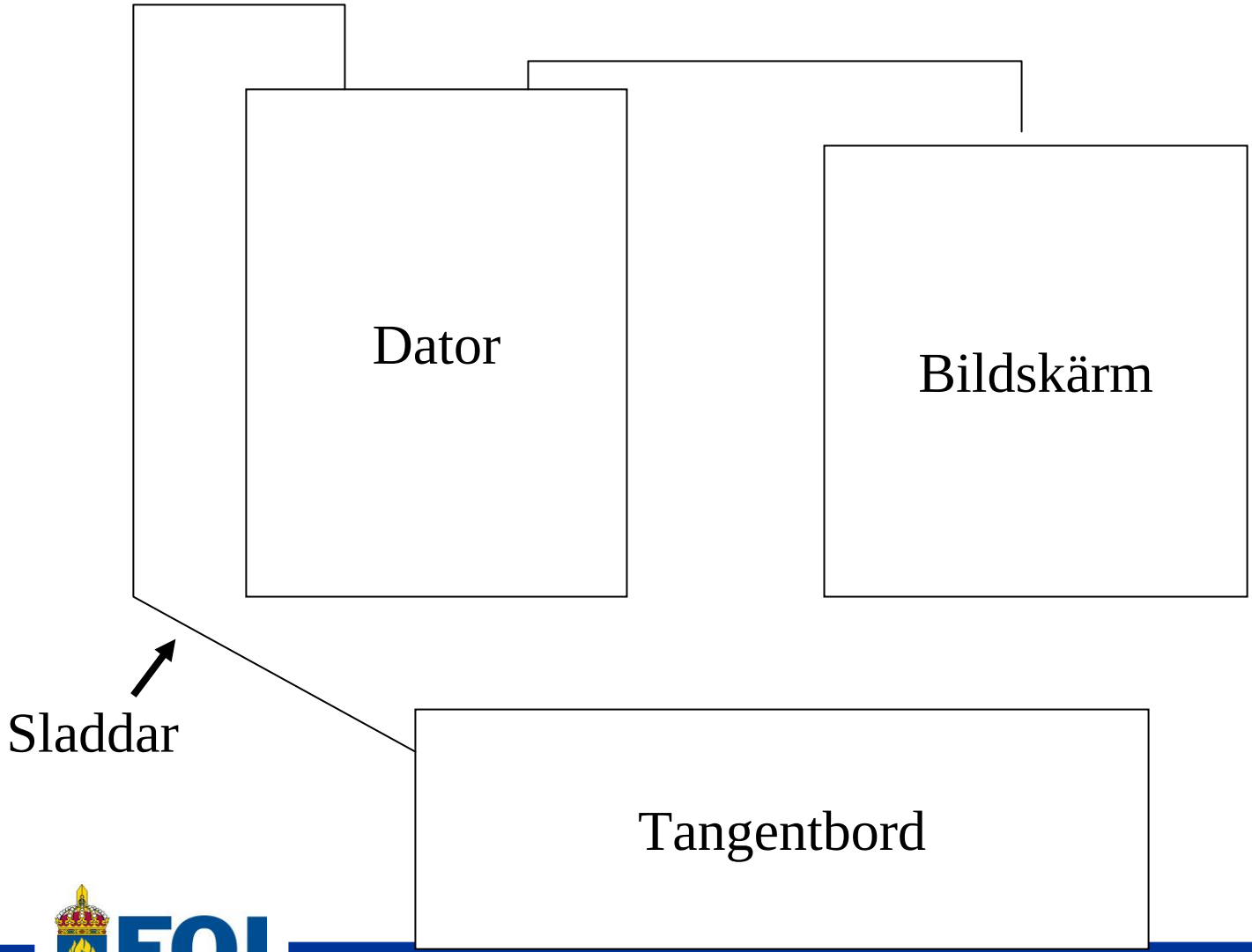
Slutsatser

- Angriparen har nu tillgång till ALLT som skrivits in på tangentbordet: Lösenord, kreditkortsnummer etc.
- Man bör säkra alla delar av kedjan, dvs även sin egen dator. En brandvägg hade stoppat just den här attacken.
- När man får en CD och ska installera saker. Se till att vara RIKTIGT säker på var den kommer ifrån.
- MEN.....

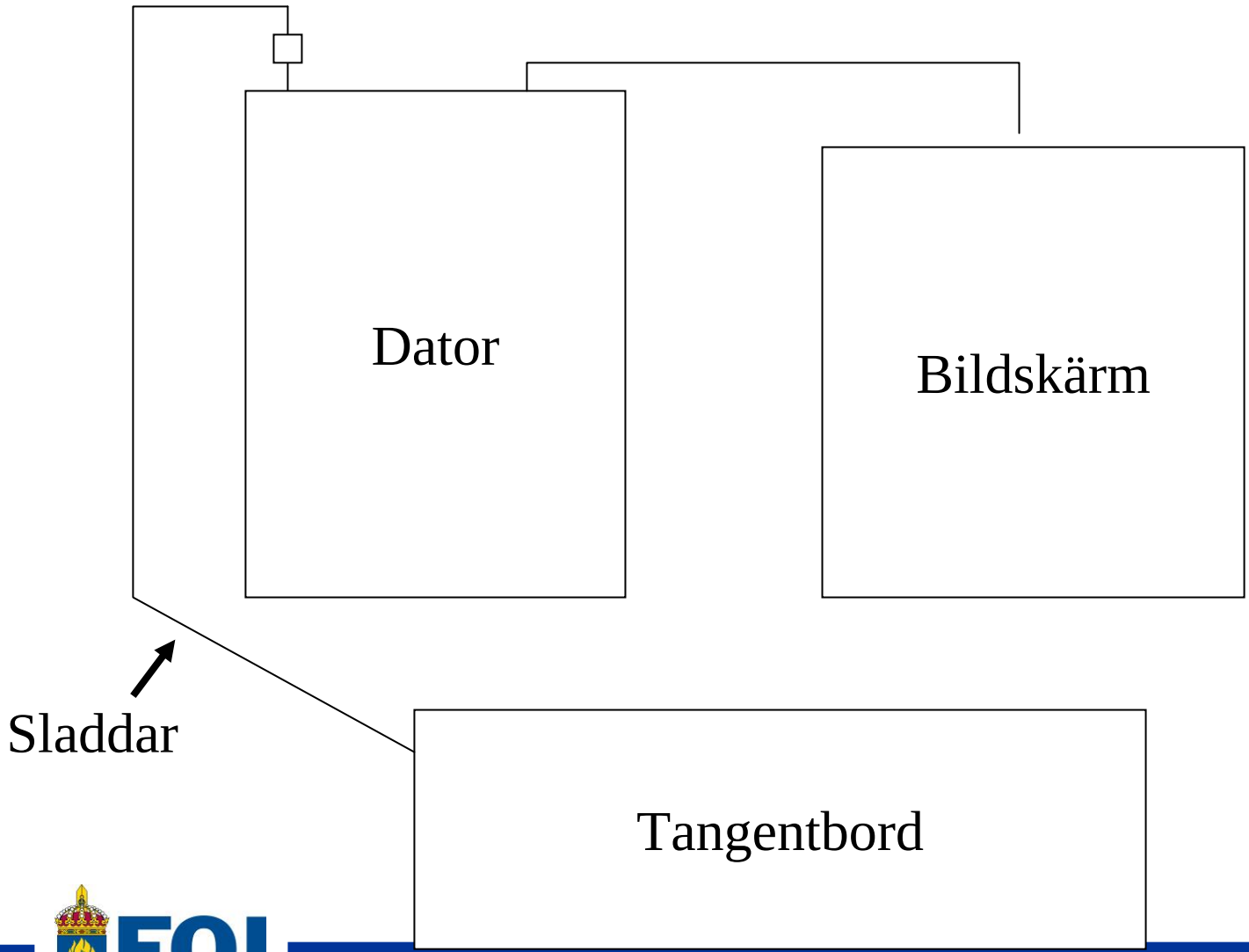
KeyGhost

- Det är väsentligt att inte fokusera så hårt på programvara och nätverkskommunikation att man glömmer de fysiska säkerhetsåtgärderna.
- Ofta har städare eller annan personal tillgång till datorutrustningen och kan koppla in eller byta ut hårdvara.

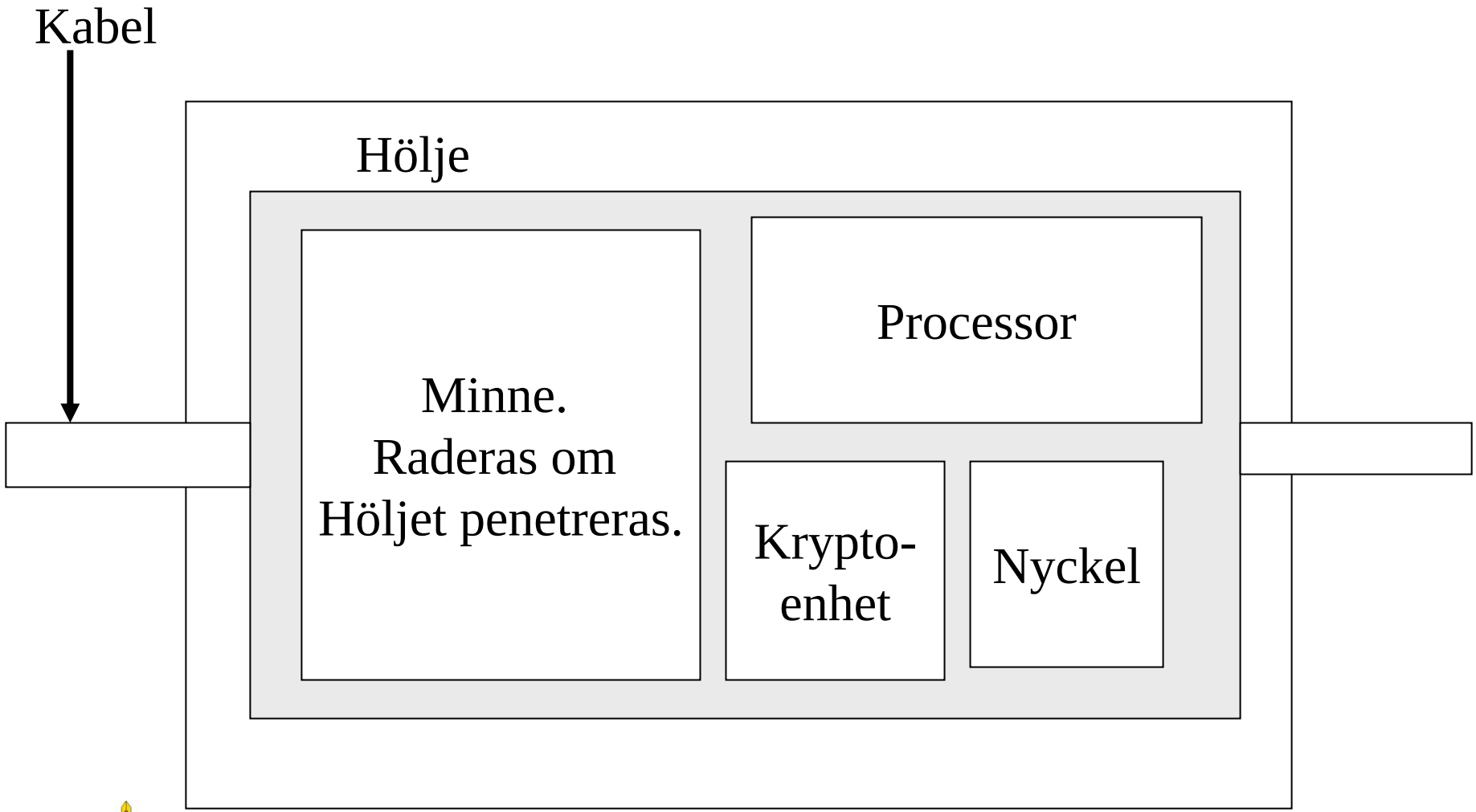
KeyGhost inledning



KeyGhost forts



KeyGhost (möjligt exempel)



Tekniska detaljer

- 512kB minne (~ ett års datoranvändning)
- Data lagras i krypterad form
- Köptes rakt över disk
- Dyrare modeller har snifferutrustningen inbakad i ändkontakten. Ser likadan ut som en förlängningssladd
- Modeller finns som har en radiosändare

Slutsatser

- Hårdvara kan modifieras till att användas för attacker p s s som programvara
- Om hårdvara manipulerats kan attacker ske oberoende av programvarorna.
- Att hitta modifierad hårdvara är oerhört svårt. (Vårt exempel är stort och klumpigt)

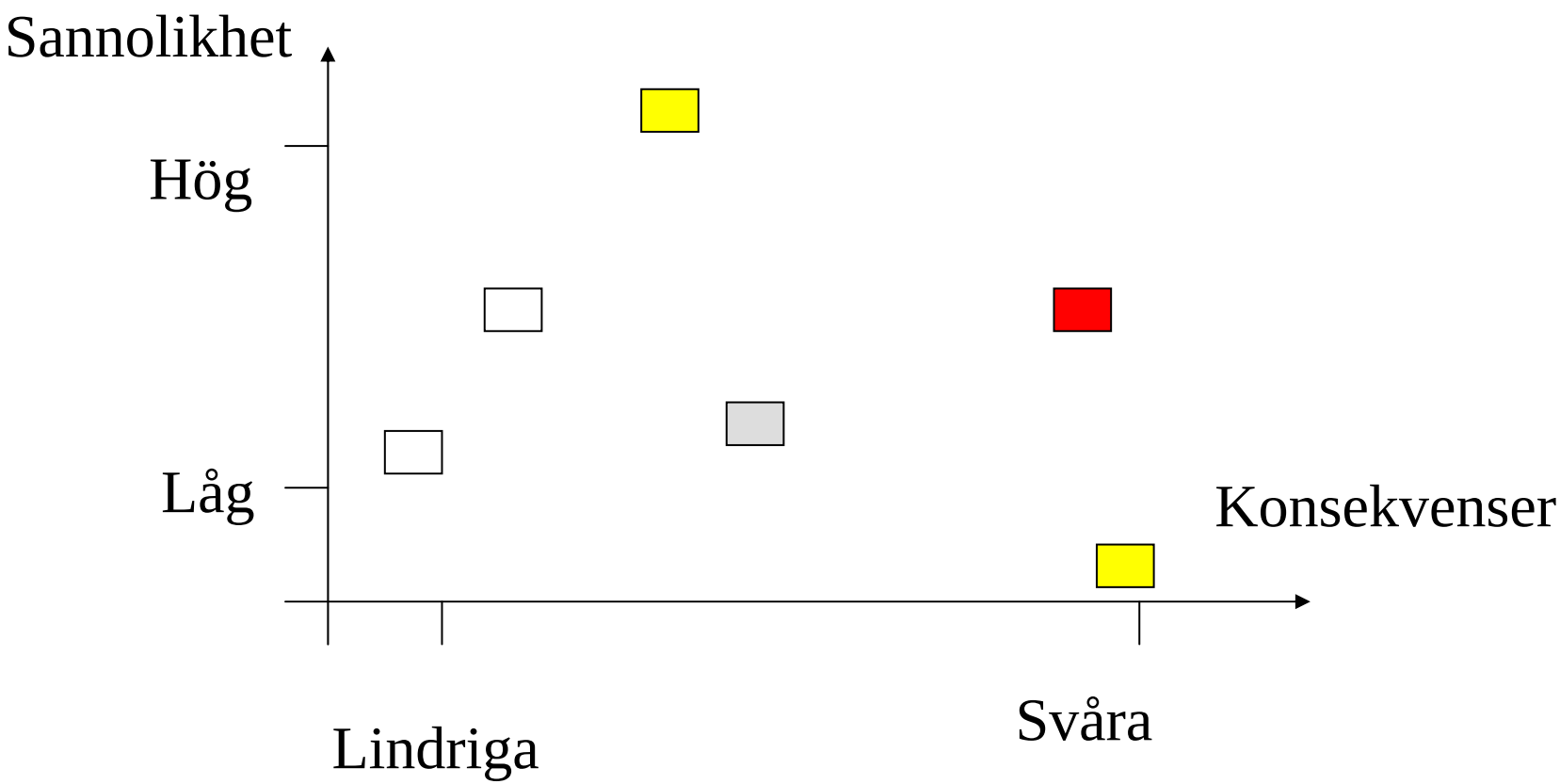
David-Besse Nuclear Power Plant 030125

Vems var felet att detta hände?

Riskanalys

- Hot
  - Oönskad händelse som kan störa verksamheten
- Brist
  - Faktum som leder till att Hot får oönskade konsekvenser
- Skada
  - En oönskad konsekvens av Hot och Brist

Riskanalys II



Riskanalys D-B

- Hot: Det finns virus och maskar på Internet
- Skada: Kärnkraftverkets kontrollsystem slutade fungera
- Vad var bristen som tillät detta?

Om de som gör analyserna inte har god kunskap om området finns en risk att man ”letar under lyktstolpen, för där är det ljust”

Frågor som inte berördes i framställningen

- Regelverk och policies?
- Ansvar för att dessa följdes?
- Utbildning hos de ansvariga?
- Resurser för inköp av utrustning,utbildning, uppföljning och kontroller?

Sammanfattning

- Informationssäkerhet är inget enkelt eller litet område. En ensam person har ingen chans att någonsin kunna lära sig allt om datasäkerhet.
- Att höja säkerheten på ett effektivt sätt i en organisation kräver bra koordinering och deltagande av experter inom olika områden.
- För att säkerhetsarbetet ska bli effektivt måste det få stöd ända från toppen i organisationen och bedrivas på alla nivåer. Det är en kontinuerlig process.
- Åtgärder är både tekniska och organisatoriska.