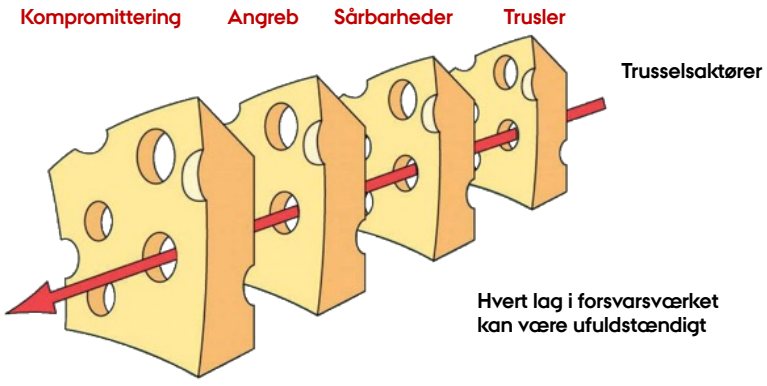
TRUSSELSMODELLERING FOR ALLE

CHRISTIAN DAMSGAARD JENSEN
PROFESSOR OF CYBERSECURITY
CDJ@ECE.AU.DK

1

TRUSLER MOD SIKKERHEDEN

Schweizisk ost modellen



Lag på lag af forsvarsværker, barrierer og sikkerhedsforanstaltninger

2

SECURITY BY DESIGN

Moderne sikkerhedsstandarder kræver en risikobaseret tilgang til cybersikkerhed

- GDPR, NIS2, CER, CRA, PLD
- ISO 27K, NIST CSF
  - ISO 27005, ISO 31000, NIST SP 800-37, IEC 62443-3-3

Generelle metoder til risikostyring indeholder mange af de samme elementer

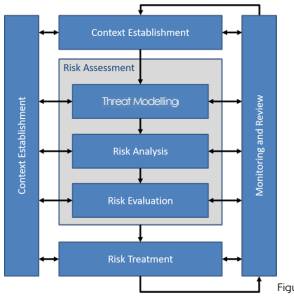


Figure: https://essif-lab.pages.grnet.gr/framework/docs/terms/pattern-decentralized-risk-management

3

FOKUS FOR TRUSSELSMODELLERING

Trusselsaktørfokus
Hvem er modstanderen?
Hvordan vil de angribe?

Systemfokus
Hvilke sårbarheder findes?
Hvad kan modstanderen opnå?

Værdifokus
Hvilke værdier skal beskyttes?
Hvordan kan de skades?

4

KLASSISK TRUSSELSMODELLERING

Trusselsmodellering identificerer uønskede hændelser

- Forstå de sikkerhedsmål man søger at realisere
- Forstå det system man forsøger at sikre
- Forstå de trusselsaktører man står overfor
- Forstå de teknikker trusselsaktørerne benytter (*angrebsvektorer*)
- Forstå de sårbarheder angriberne udnytter
  - Summen af angrebsvektorer kaldes angrebsoverfladen
- Forstå hvilke modforholdsregler der er effektive mod disse angreb

Kendte teknikker inkluderer STRIDE, PASTA, OCTAVE og Attack Trees

- Vi ser kort på STRIDE og Attack Trees i det efterfølgende

5

TRUSSELSMODELLERING I PRAKSIS (5 TRIN)

1. Identifikation af sikkerhedsmål
   - Typiske mål er fortrolighed, integritet og tilgængelighed (CIA)
2. Model af systemet
   - Hvad skal systemet kunne, hvem skal bruge det og hvordan?
3. Identifikation af elementer i systemmodellen
   - Enkeltstående moduler, med grænseflader (API'er)
   - Kommunikationskanaler og datastrømme
4. Identifikation af trusler
   - Se på standard angrebsteknikker
5. Identifikation af sårbarheder
   - Analysere systemet for sårbarheder der kan udnyttes
   - Se på motiv, evne og mulighed

6

TRUSSELSMODELLERINGSMODELLERING

Trusselsaktør
- Evne
- Motiv
- Mulighed

Angrebs vektorer
- TTP
- IOC (signaturer)

Systemer (Værdier)
- Sårbarheder
- Pentest

Threat Intelligence
Reports & Services

Cyber Kill Chain
MITRE
- ATT@CK
- CAPEC
- Attack Flows

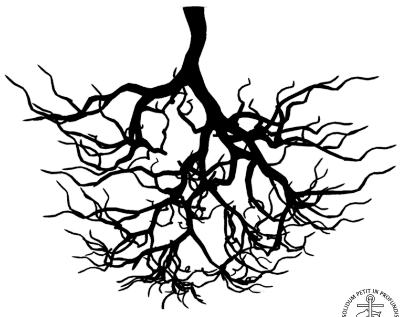
CVE/CVSS
CWE/CWSS
CISA KEV
Threat Intelligence
Inkl. fortegnelser over computere og netværk

7

ATTACK TREE MODELLEN

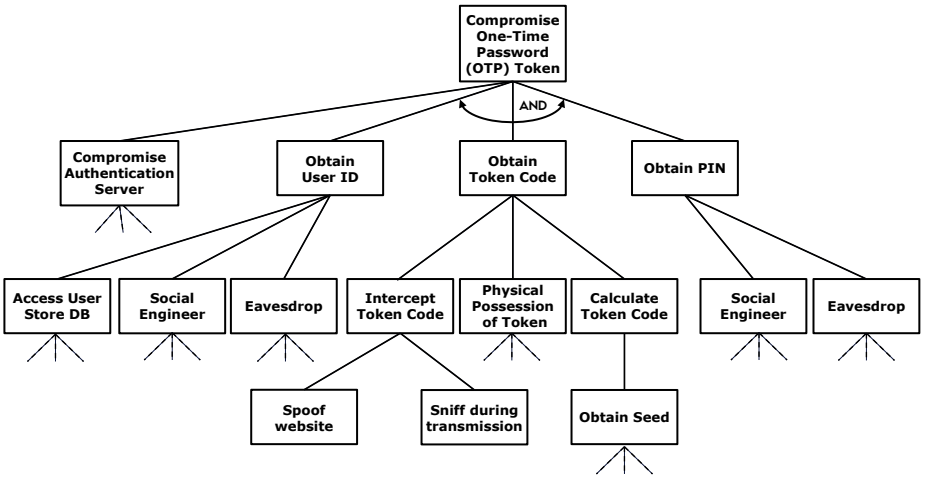
Attack trees tager udgangspunkt i angriberens mål
- Metodisk gennemgang af måder angriber kan opnå sine mål
- Kræver at man fårstår angriberens motiv, evne og mulighed for angreb
- Bygger på "Fault trees" der er en velkendt abstraktion

Attack trees repræsenterer alle angriberens delmål som et træ
- Hovedmålet udgør træets rod, som sædvanligvis er opad



8

EKSEMPEL PÅ ET "ATTACK TREE"



9

STRIDE MODELLEN

Spoofing
- agenter udgiver sig for at være en anden

Tampering
- uautoriserede ændringer af systemer eller data

Repudiation
- agenter nægter at have send en besked eller udført en handling

Information leakage
- fortrolighed brydes fordi information lækkes til udenforstående

Denial of Service
- systemer eller data gøres utilgængelige for autoriserede brugere

Elevation of Privilege
- agenter opnår højere privilegier, f.eks. administratorrettigheder

10

MODELBASERET TRUSSELSMODELLERING

Det kan være svært at forstå angriberne og deres metoder

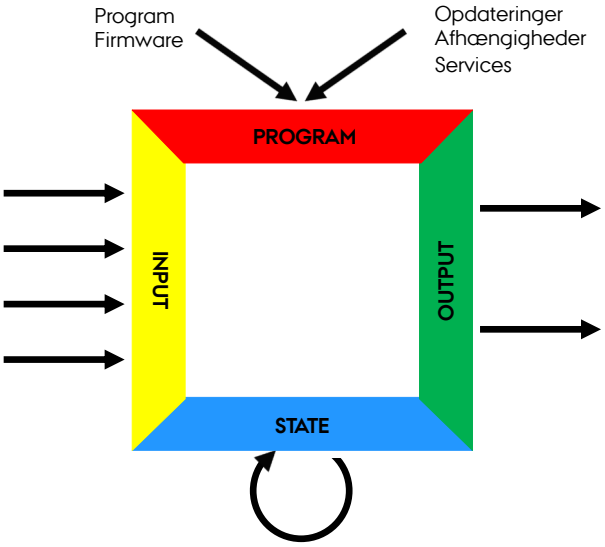
I stedet tager vi udgangspunkt i en detaljeret produktbeskrivelse

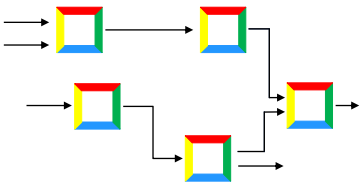
- Systemudviklerne kan benytte specifikationen
- System indkøbere kan bruge svar på udbud/salgsmateriale/datablade

Krævet ikke særlig viden om sikkerhed, men nært kendskab til systemet

11

GENERISK SYSTEM MODEL





12

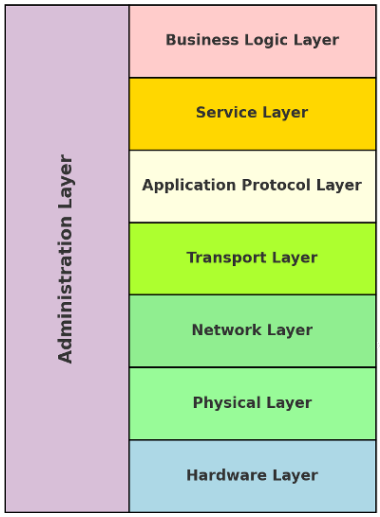
GENNEMGANG AF HVER KOMPONENT

Begynd med det du kan se (hardware)

- Stik, porte, antenner, ...
- Konsulter specifikationer, manualer, datablade, ...
- Kig i kassen (hvis det er muligt)

Fortsæt opad i stakken når hardware er identificeret

- Hvilke muligheder muliggøres på hvert lag
  - input, output, kontrol/services, state manpulation

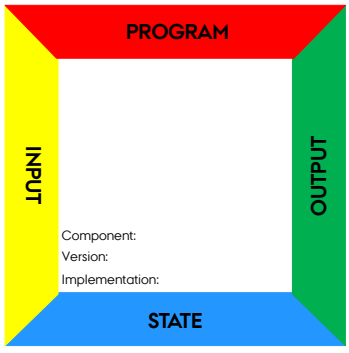


15

Layer:

Control Input	Implementation

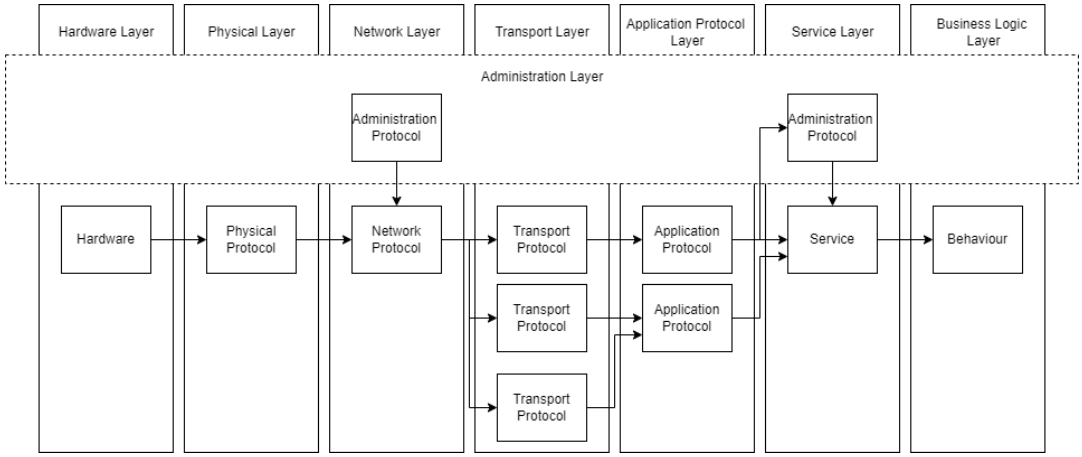
Input



Output

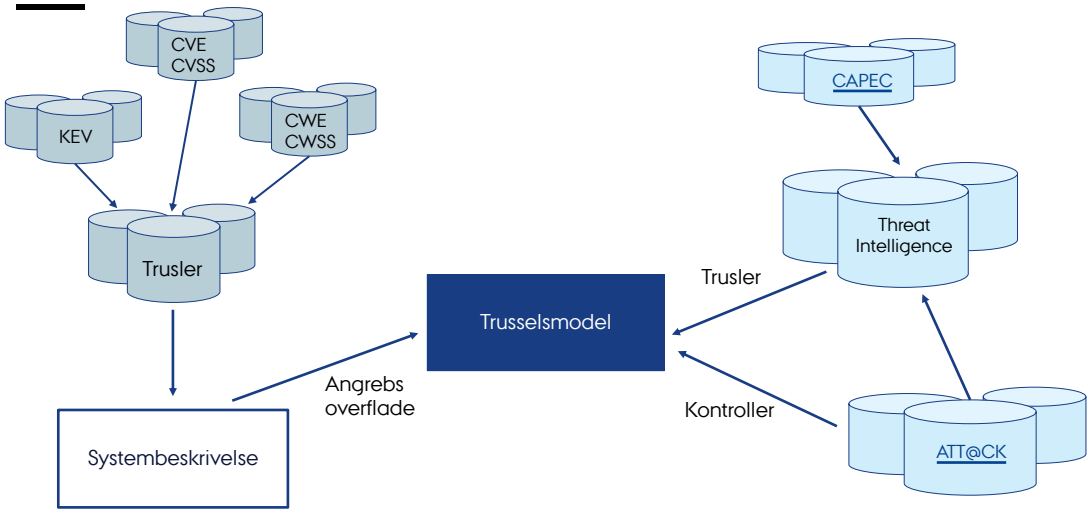
16

SAMLET DÆKNING AF TRUSLER



17

AUTOMATISERING AF TRUSSELSANALYSEN



18

EKSEMPEL PÅ TRUSSELSANALYSE

19

TRUSSELSANALYSE AF SOUNDBOKS

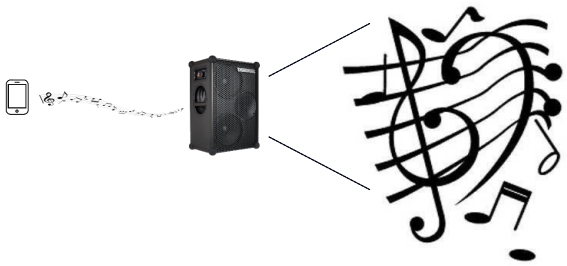
1. Identificer sikkerhedsmål
   - Konfidentialitet: ???
   - Integritet: musikafspilning, kontrol (volumen), konfiguration, ...
   - Tilgængelighed: musikafspilning, kontrol
2. Byg model af systemet
3. Dekomponer modellen
4. Identificer trusler (Hvad betyder **S T R I D E** i denne sammenhæng?)
5. Identificer sårbarheder

20

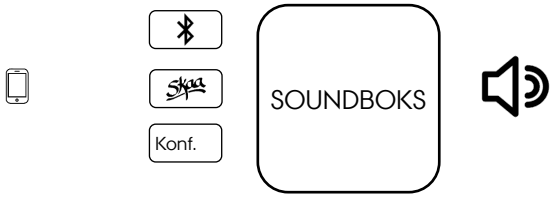
TRUSSELSANALYSE AF SOUNDBOKS

MODELLERING AF SOUNDBOKS

Systemmodel



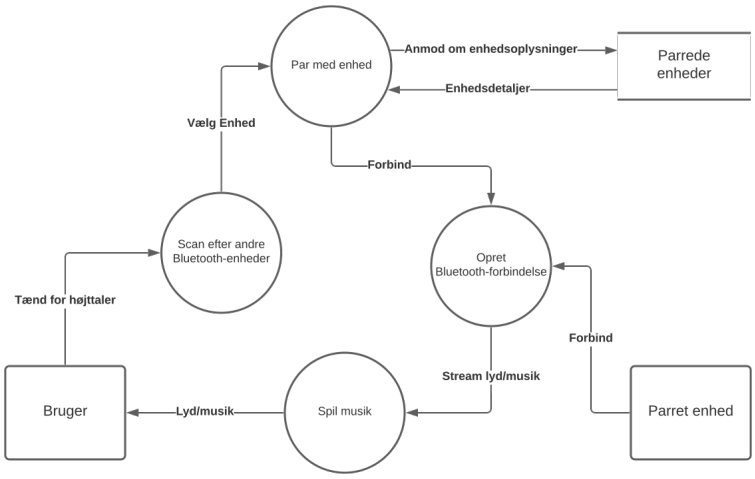
Elementer af modellen



21

TRUSSELSANALYSE AF SOUNDBOKS

DATA FLOW DIAGRAMMER



22

TRUSSELSVURDERING

STRIDE per element tager udgangspunkt i de elementer man har identificeret i DFD'en

	Element	Interaction	S	T	R	I	D	E
1	BT forbindelse	Parring mellem telefon og Soundboks	X				X	
2		Afspilning af musik	X	X			X	
3		Kontrol af Soundboks (tænd/sluk, volumen, ...)	X	X			X	x
4								

#1 Parring mellem telefon og soundboks

S Spoofing kan tillade uautoriserede telefoner at parres med Soundboks eller at telefon parres med uautoriseret Soundboks

D Ovenstående angreb tillader direkte Denial of Service, ved at slukke for boksen, skrue ned for lyden eller spille noget helt andet, men hvis parring kan brydes (deautentifikation) resulterer det også i DoS

23

AARHUS UNIVERSITY

24