Cloud security
Virtualisering
Serverless security
IoT security
AI security
Hardware security
Physical security

Carsten Jørgensen
Department of Computer Science

DIKU 23. september 2019

Old School vs. New World


En cloud…

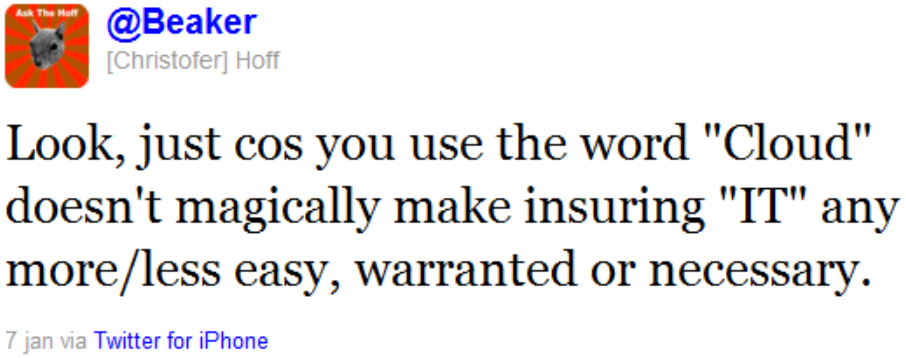

En cloud...

Hvad skal man tænke på?

”Cloud” er ikke automatisk ”sikkert”

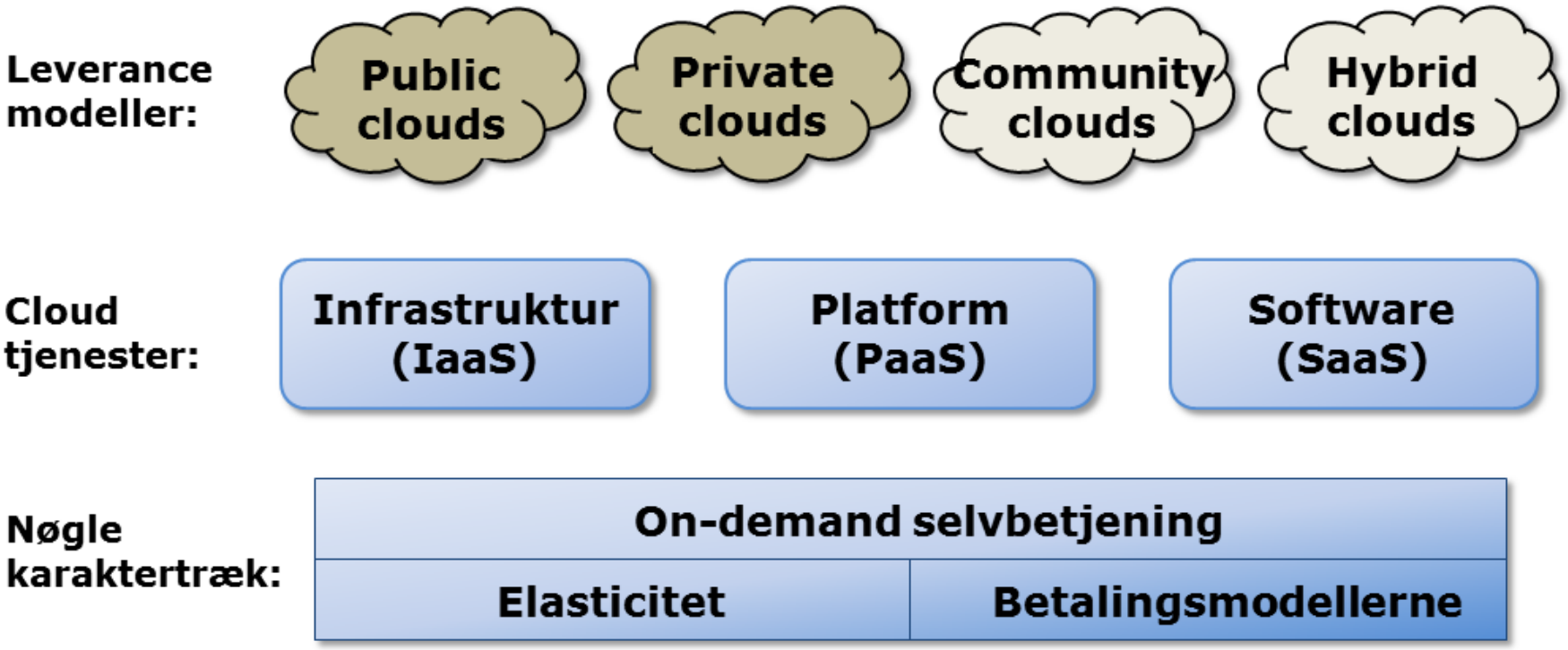
IT bliver ikke ”sikkert” på magisk vis, bare fordi man kalder noget ”cloud”

Men det bliver heller ikke usikkert



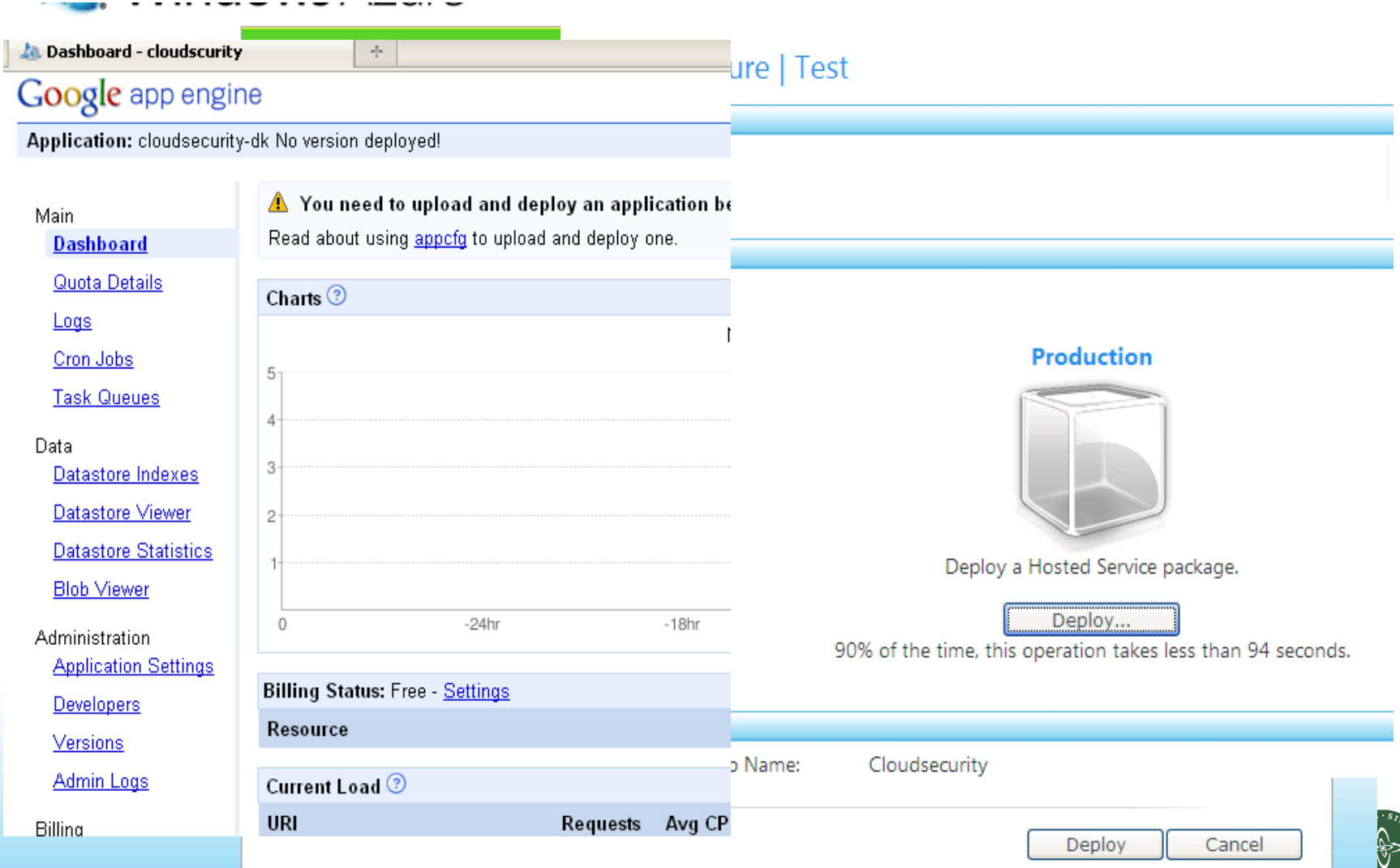
Hvad er cloud computing

Cloud Computing er en drifts- og leverancemodel

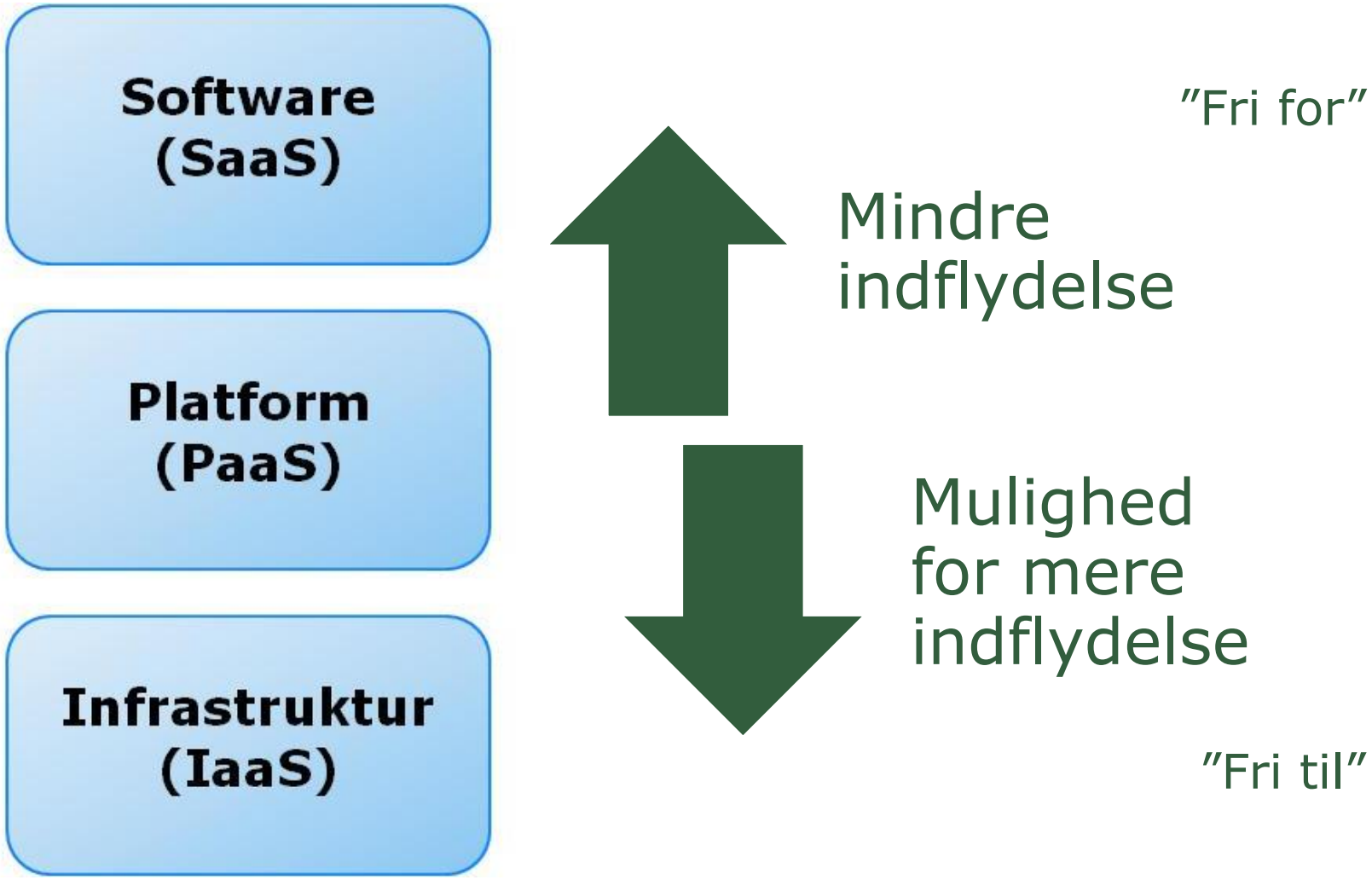


IaaS: Ops without hardware
PaaS: Devs without Ops
SaaS: Business without Devs

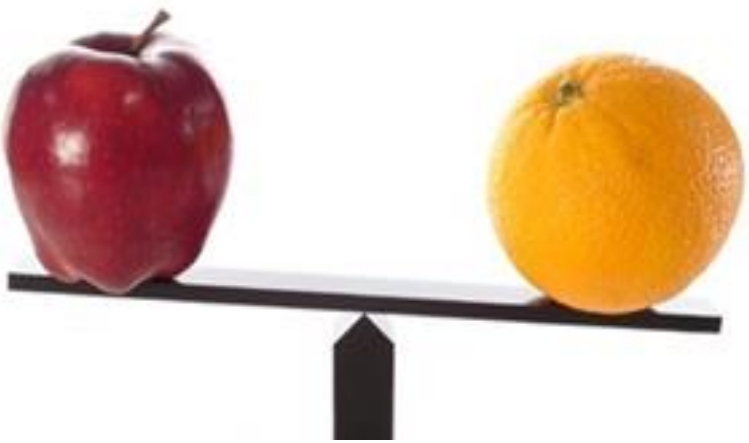
Platform as a Service



De tre *aaS modeller



Hvad er den bedste cloud løsning ?



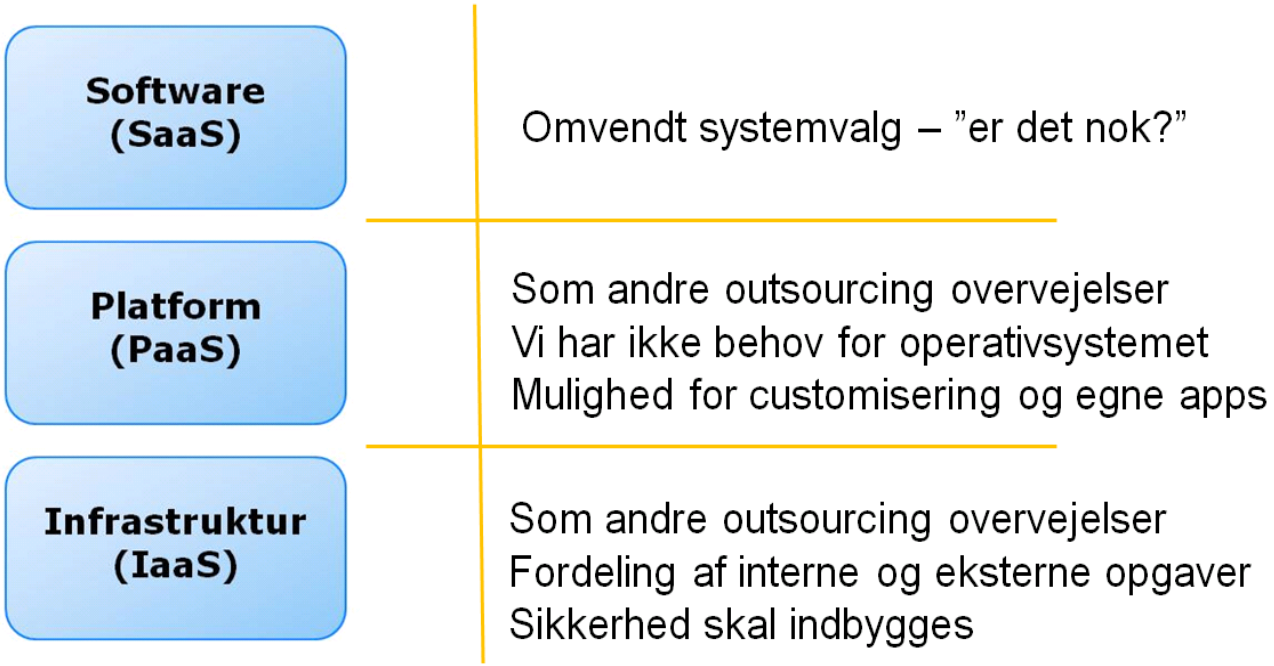
Cloud Computing er ikke én specifik arkitektur eller én teknologi, det er en driftsmodel

Delt ansvar...

Løsning:	Eget ansvar:	Cloud-leverandørs ansvar:
Software (SaaS)	Konfiguration af log	Data Applikationer
Platform (PaaS)	Logs fra egne apps	System Management
Infrastruktur (IaaS)	Lokal overvågning Applikationslogs OS logs	Netværk Hardware, host Procedurer m.m. Fysisk sikring

Overvejelserne

De fleste overvejelser i forbindelse med outsourcing gælder også for cloudsourcing



Traditionel sikkerhedsmodel med compliance hensyn

Risiko vurdering

+

Data klassifikation

Er vi underlagt lovkrav ?
Vores sikkerhedsmodel

Persondatalovgivningen
Bogføringslovgivningen
SOX
Euro-SOX
PCI
ISO 27001
…

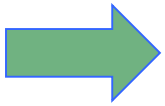
Arbejdsgang

Lovkrav:
Persondatalovgivning
Regnskabsloven

Compliance hensyn:
PCI
SOX

Sikkerhedsmodel:
DS484
ISO 27002

Risiko vurdering
+
Data klassifikation



Software (SaaS)

Applikationer

Data

Platform (PaaS)

System Management

Infrastruktur (IaaS)

Netværk

Hardware

Fysisk sikring

Fysisk placering

Cloud risikovurdering

Failure Mode	Probability	Mitigation Plan
Application Failure	High	Automatic degraded response
AWS Region Failure	Low	Wait for region to recover
AWS Zone Failure	Medium	Continue to run on 2 out of 3 zones
Datacenter Failure	Medium	Migrate more functions to cloud
Data store failure	Low	Restore from S3 backups
S3 failure	Low	Restore from remote archive

??

Men ikke meget anderledes

POLITIKEN.DK

KØBENHAVN LIGE NU: 1°
Vejret næste 10 døgn
Vejret i andre byer

OPRET

Skriv dit søgeord

NYHEDER | KULTUR | SPORT | DEBAT | IBYEN | TJEK | TUREN GÅR TIL | POLITIKEN TV | FOTO | NEWS | BAGSIDEN | HELT NORMALT

NYHEDER | Danmark | Politik | Internationalt | Erhverv | Klima | Videnskab | Uddannelse | 48 timer

KRISTIAN MADSEN: Socialdemokratisk idékrise indtil 2032

IBYEN-PRISEN: De fem nominerede til Årets Begivenhed

FORSKERE: Her er de gener, som kan gøre dig 8 kilo tykkere

INDSA
sårede
bidrag

DANMARK 1. JUN. 2011 KL. 11.22 OPDATERET 1. JUN. 2011 KL. 11.54

Strømmen forsvundet i hele Københavns indre by

Højspændingsfejl giver store driftsforstyrrelser.

Annonce

LAVPRISKALENDEREN
Afgang
Copenhagen (CPH)
Destination
-Vælg destination-
Søg
norweglan.com

SENESTE NYT

1 2 3 FACEBOOK SEND PRINT TIP OS

AF **KAARE SKOVMAND**

Store dele af København er lige nu helt uden strøm.

Årsagen er en større driftsforstyrrelse i en transformator, der ifølge DONG Energy tidligst kan forventes udbedret inden for to timer.

Uheldet skaber lige nu store problemer for trafikken.

Annoncer

KØBENHAVNS UNIVERSITET

Ikke magi

Det er ikke nødvendigt at starte forfra på cloud sikkerhedsarbejdet, mine sikkerhedskrav er (nok) ikke unikke

ISACA
Trust in, and value from, information systems

amazon web services™

Google Apps

cloud security alliance
CSA

Windows Azure

salesforce

enisa
European Network and Information Security Agency

ISF Information Security Forum

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

cloudsecurityalliance.org

RESEARCH INITIATIVES ↘

CCM™

Cloud Controls Matrix
Security controls framework for cloud provider and cloud consumers

CAI™

Consensus Assesments Initiative
Research tools and processes to perform consistent measurements of cloud providers

Cloud Audit™

Cloud Audit
Forum in which providers can automate the Audit, Assertion, Assessment, and Assurance (A6) of IaaS, PaaS, and SaaS environments.

CTP™

Cloud Trust Protocol
The mechanism by which cloud service consumers ask for and receive information about the elements of transparency as applied to cloud service providers.

Cloud SIRT

CloudSIRT
Enhance the capability of the cloud community to prepare for and respond to vulnerabilities, threats, and incidents in order to preserve trust in cloud computing.

Security Guidance for Critical Areas of Focus in Cloud Computing
Foundational best practices for securing cloud computing

Cloud Metrics
Metrics designed for Cloud Controls Matrix and CSA Guidance

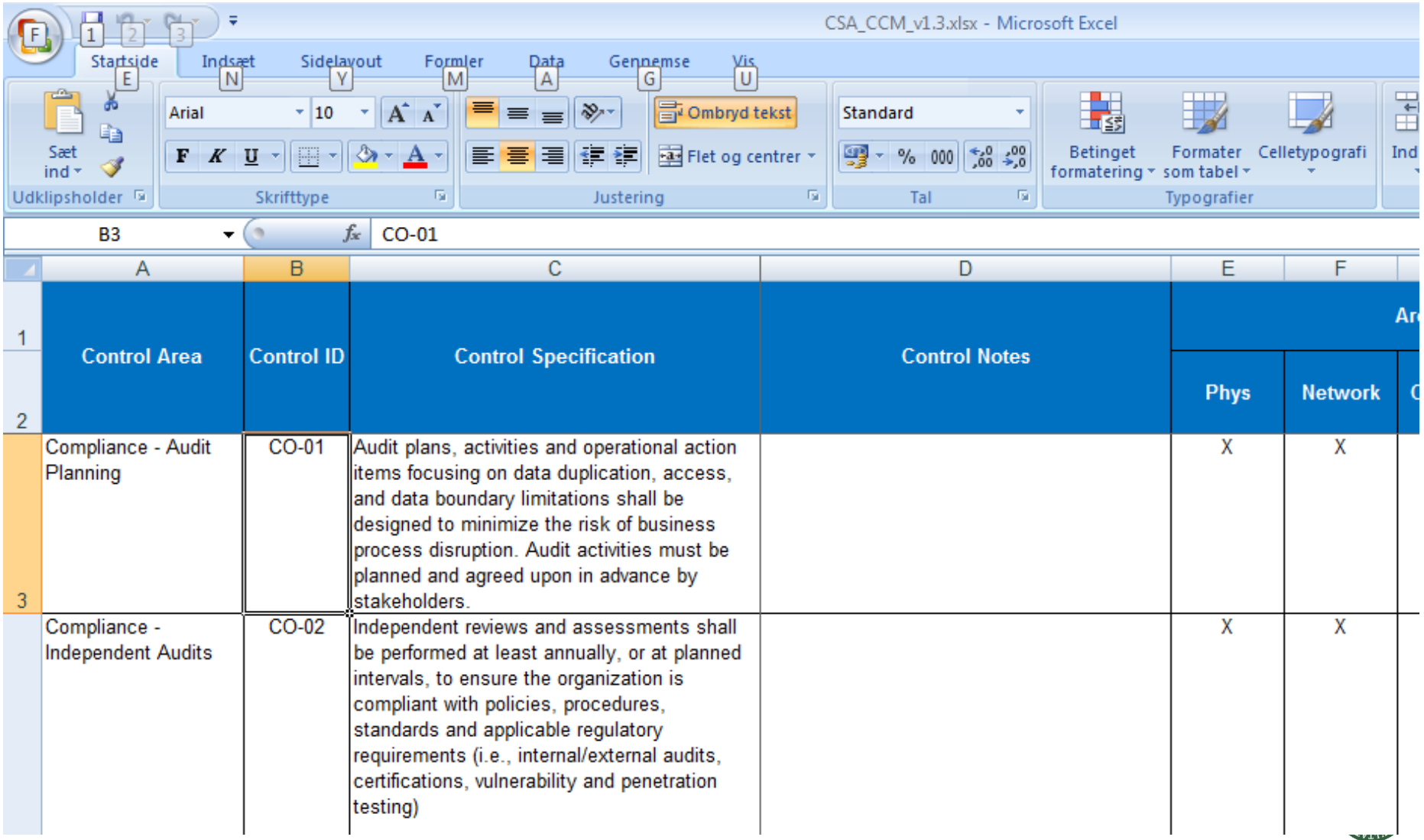
Trusted Cloud Initiative
Secure, interoperable identity in the cloud

Common Assurance Maturity Model
Benchmarks capabilities to deliver information assurance maturity of specific solutions.

Top Threats to Cloud Computing
Threat research updated twice yearly

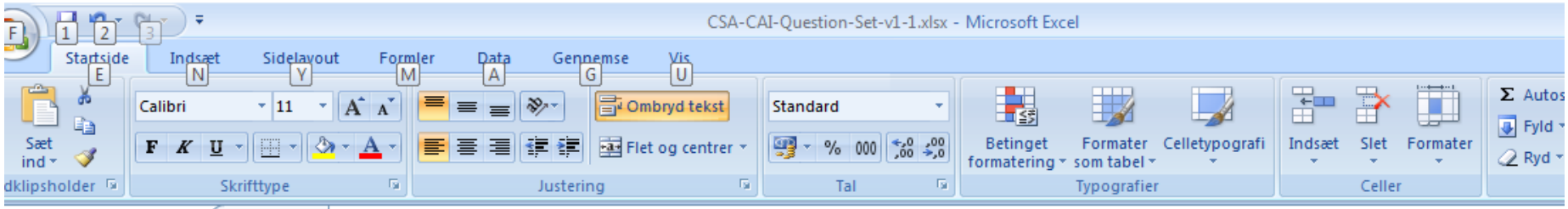
CSA GRC Stack
integrated suite of 3 CSA initiatives: CloudAudit, Cloud Controls Matrix, CAI Questionnaire

Cloud Audit – Cloud Controls Matrix



	A	B	C	D	E	F
1	Control Area	Control ID	Control Specification	Control Notes		
2					Phys	Network
3	Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.		X	X
	Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)		X	X

Cloud Audit – Consensus Assessment Initiative



C	D	E	F	G
Consensus Assessments Initiative Questionnaire v1.1				CCMv1.1 C
Control Group	**CGID**	**CID**	**Consensus Assessment Questions**	**Comments and Notes**	**COBIT**
Compliance					
Audit Planning	CO-01	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?		COBIT 4.1 2.2 PO 9.5
Independent Audits	CO-02	CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?		COBIT 4.1 ME2.5, ME
		CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?		
		CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?		
		CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?		
		CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?		
		CO-02.6	Are the results of the network penetration tests available to tenants at their request?		
		CO-02.7	Are the results of internal and external audits available to tenants at their request?		
Third Party Audits	CO-03	CO-03.1	Do you permit tenants to perform independent vulnerability assessments?		COBIT 4.1 2.1, DS 2.4
		CO-03.2	Do you have external third-party conduct vulnerability scans and periodic		

cloudsecurityalliance.org/star/registry

CSA STAR Security, Trust & Assurance Registry

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Acquia

http://www.acquia.com

Acquia offers enterprises unparalleled freedom to innovate and increase business agility by creating extraordinary web experiences. The fastest growing open cloud platform for integrated digital experiences, Acquia enables content rich, complex global organizations to rapidly deploy and manage dynamic digital experiences in an open source way. Co-founded by the Drupal project's creator in 2007, Acquia...

Read More..

Self-Assessments

CAI Questionnaire

Download

Submission Info

Date Listed: January 12, 2013

Amazon AWS

https://aws.amazon.com/

amazon web services™

Amazon Web Services provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. With data center locations in the U.S., Europe, Brazil, Singapore, and Japan, customers across all industries are taking advantage of the following benefits: Low Cost, Agility and Instant...

Self-Assessments

CAI Questionnaire

Download Instructions:

Go to aws.amazon.com/security

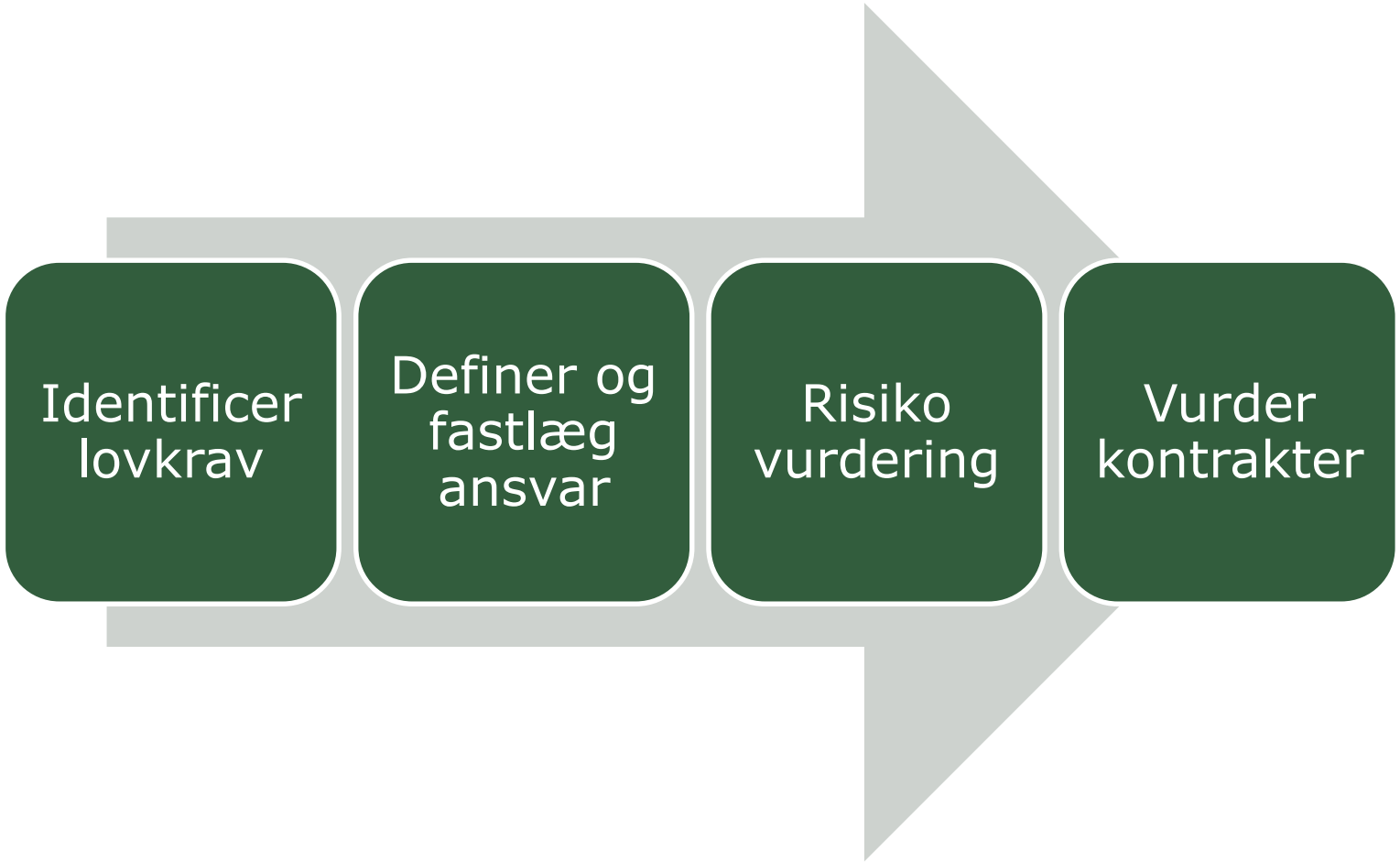
Select Amazon Web Services: Risk and Compliance whitepaper (pages 15-38)

PGP Signature

Download

Submission Info

Interne cloud krav



Kan jeg få den i grøn?

IKEA®

Plads til livet

Søg

Sortiment | Nyheder | Dagligstue | Soveværelse | Køkken | Børnenes

MALTE

Bartaburet

kr 229 / stk.

rød
sort

Prisen afspejler det valgte

”Cloud”, cloud eller CLOUD

eller

”Cloud” og cloud – traditionel outsourcing eller cloudsourcing

Standardisering

Ingen IT i 12 timer :)

Clouds er forskellige

Hi all!

We wanted to send you a quick message to let you know that on the 15th of February, 2014, from 8:00 a.m. till 8:00 p.m. EST, Verizon Cloud will receive a number of software updates. We wanted to give you plenty of lead time as your virtual machines will not be available during the twelve-hour upgrade window and we wanted to minimize the inconvenience to you. Before the window, please login to your environment and power down your VMs. As always, please don't hesitate to contact us with any questions or concerns. We'll let you know when the upgrades are complete. :)

Verizon Cloud Client Care
We're available 24/7
Toll free (U.S.): 1-855-338-1427
Toll: +1 (469) 461-9722
Email: vzcloudhelp@verizon.com

Baby skyer

KMD bygger en sky, der skal huse 10.000 servere i 2017

Enterprise architect Thomas Lervig Struer ved én af de switches, der forbinder serverne og de enkelte pods med hinanden i KMD's nye sky.

I den ene af KMD's maskinstuer står den sky, der er fremtidens platform for it-

Sikkerhed i skyen

Alle de kendte sikkerhedsudfordinger findes i skyen

Din kontrakt

Det er **DIT** ansvar at vælge en leverandør, der leverer den fornødne grad af teknisk sikkerhed og forsvarlige procedurer, og det er **DIT** ansvar at kontrollere overholdelsen af det aftalte.

Data i EU — Patriot Act, FISAA…

Brugen af kryptering

Leverandørens muligheder for adgang til din data

Logning

Sletning af data

Kassering af datamedier

Revisorerklæring om datasikkerheden

Hovedsaligt valg af certificerede leverandører
(lige nu primært ISO 27001)

Registreredes rettigheder

Cloud sikkerhed >< traditionel it-sikkerhed

- ”Design for failures” – forvent service issues
- Opdater og udrul nye instanser, ikke de kørende
- Paranoid arkitektur: opdel services
- Kryptering, data at rest

IaaS-løsninger:
Det kan være let at bruge bastion/jump hosts til al adgang
Eller etablerer ”read-only logging via oneway tunnel”

Cloud sikkerhed og traditional sikkerhed

To-faktor adgang, flere niveauer

Brug af begrænsede konti fra starten, også i cloud

Brug forskellige sikkerhedsgrupper, adskilte admingrupper og sikkerhedsgrupper

Hvad sker der når cloud-løsningen fejler

Single Point of Failures og afhængigheder ved kombineret infrastruktur

- Availability
- Laveste fællesnævner
- Delvis tilgængelighed

Security Issues for Cloud Computing

Security is a major consideration when augmenting or replacing on-premises systems with cloud services

Allaying security concerns is frequently a prerequisite for further discussions about migrating part or all of an organization's computing architecture to the cloud

Availability is another major concern

Auditability of data must be ensured

Businesses should perform due diligence on security threats both from outside and inside the cloud

- Cloud users are responsible for application-level security
- Cloud vendors are responsible for physical security and some software security
- Security for intermediate layers of the software stack is shared between users and vendors

Cloud providers must guard against theft or denial-of-service attacks by their users and users need to be protected from one another

Businesses should consider the extent to which subscribers are protected against the provider, especially in the area of inadvertent data loss

We are experiencing massive demand on our support capacity, we are going to get to everyone it will just take time.

Code Spaces : Is Down!

Dear Customers,

On Tuesday the 17th of June 2014 we received a well orchestrated DDOS against our servers, this happens quite often and we normally overcome them in a way that is transparent to the Code Spaces community. On this occasion however the DDOS was just the start.

An **unauthorised** person who at this point who is still unknown (All we can say is that we have no reason to think its anyone who is or was employed with Code Spaces) had gained access to our Amazon EC2 control panel and had left a number of messages for us to contact them using a hotmail address

Reaching out to the address started a chain of events that revolved arount the person trying to extort a large fee in order to resolve the DDOS.

Upon realisation that somebody had access to our control panel we started to investigate how access had been gained and what access that person had to the data in our systems, it became clear that so far **no** machine access had been achieved due to the intruder not having our Private Keys.

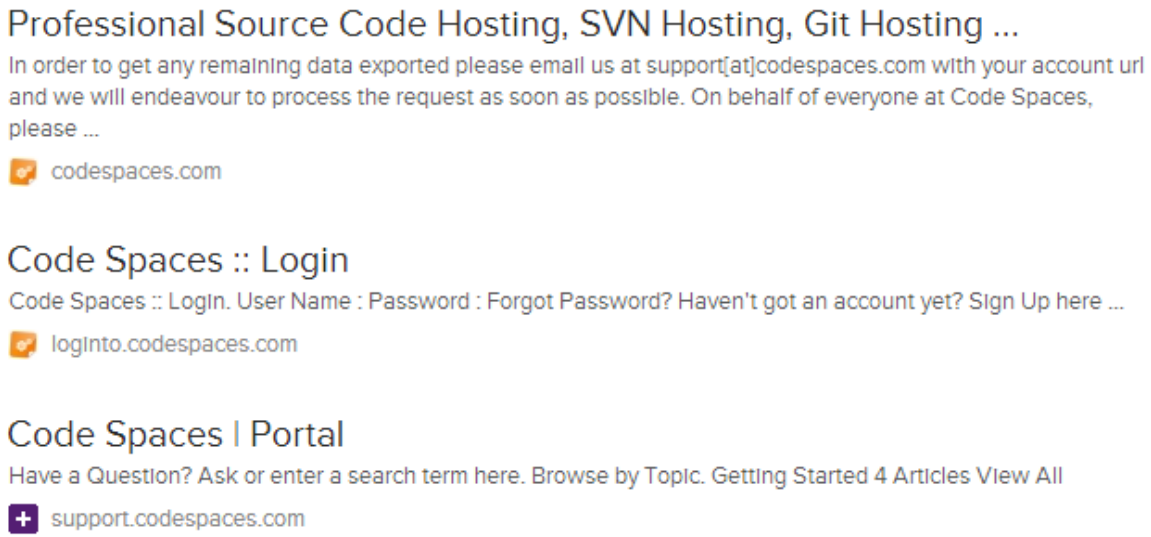
At this point we took action to take control back of our panel by changing passwords, however the intruder had prepared for this and had already created a number of backup logins to the panel and upon seeing us make the attempted recovery of the account he proceeded to randomly delete artifacts from the panel. We finally managed to get our panel access back but not before he had removed all EBS snapshots, S3 buckets, all AMI's, some EBS instances and several machine instances.

In summary, most of our data, backups, machine configurations and offsite backups were either partially or completely deleted.

This took place over a 12 hour period which I have condensed into this very brief explanation, which I will elaborate

Codespaces.com

The attacker deleted
"all machine [VMs], all EBS vols containing database files, all snapshots & backups, and all S3 data".



Codespaces.com – some lessons

- Avoid using the master credential, use the Identity Management console
- Use Two Factor Authentication: http://aws.amazon.com/iam/details/mfa/
- Segment backup access from the rest of the infrastructure. For instance backups could be archived into a different AWS account without delete access.
- Be careful about the "I forgot my password" feature.

Husk Security Groups

Åben kun for adminitrativ adgang til Security Groups når der er brug for det - fjern efter brug.

Betyder en angriber skal opnår adgang på cloud-administrations niveau OG have credentials for at kunne tilgå servere.

Næsten umuligt i traditional infrastruktur. Traditionelle firewalls for dyre og administration umuligt på det niveau.

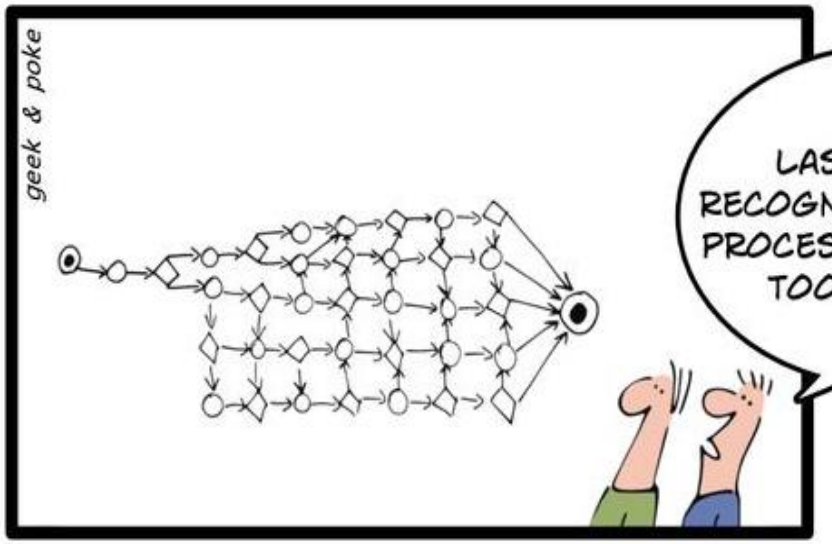
Eksempel hvor cloud kan give langt bedre sikkerhed som default.

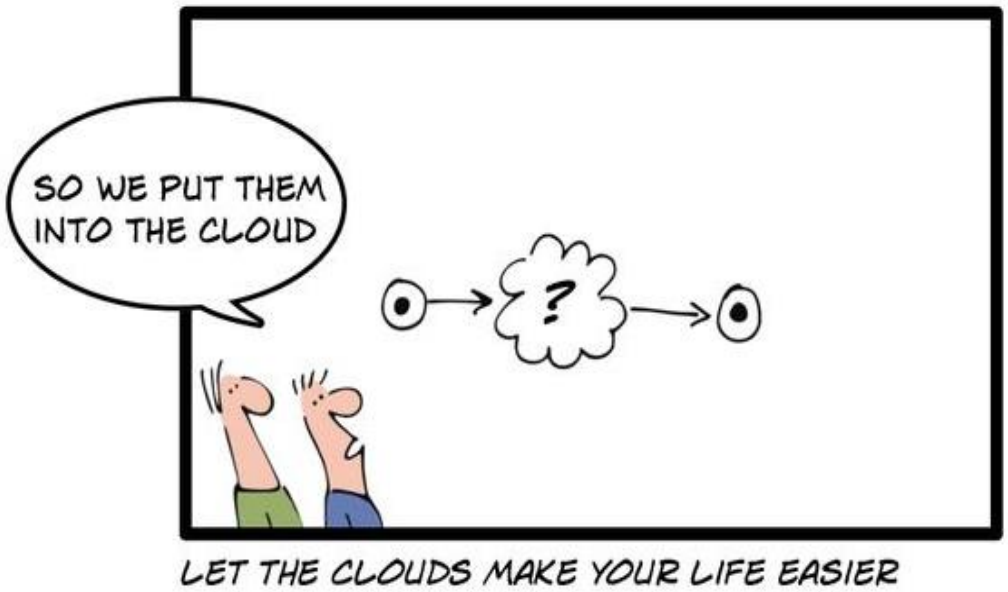
Du kan IKKE gøre skyen sikker

Men – med mindre du arbejder for en cloud-leverandør – skal du heller ikke.

Du skal kunne sikre dine **data** og dine **applikationer**

Let the clouds make your life easier





Cloud Computing er helt normale it-systemer, der bruger strøm.

It-systemer fejler en gang imellem, men de kan vurderes.

Cloud termer - Abstraction

"Abstraction" adskiller ressourcer for den underliggende infrastruktur.

Hele cloud infrastrukturen administreres over webinterfaces og API'er.
Remote control over infrastrukturen.

Cloud termer - Automatisering

Automation bruger ”*orchestration* technologies” til ressource provisionering og konfiguration, baseret på politikker.

Dynamiske servere kommer og forsvinder on-demand. Manuelle sikkerhedskontroller kan ikke følge med.

Synlighed fordi orkestreringslaget altid ved hvor alting er og hvordan det er konfigureret.

Automatisering af security compliance.

Cloud Security - termer

"Immutable Servers": Er det muligt at rule nye opdaterede instance ud istedet for at patche kørende instance. Kan gøres på live applikationer med brugere forbindet.

Snapshots: Backup af alt data uden at lukke systemet ned eller påvirke performance. Snapshots kan flyttes, også ud af skyen.

Software Defined Security: Sikkerhed kan bruge same API'er og same featuers til at automatiserer sikkerhedskontroller.
Nye servere kan automatisk deployes med sikre konfigurationer og man kan lynhurtigt skabe overblik over alle enheder.

Kubernetes/Docker/Chef/Puppet

Indsæt automatisk security agents i alle viruelle maskiner efterhånden som de starter op. Forbinder og konfigurer sig automatisk baseret på politikker.

Kan automatisk konfigurere host-based sikkerhed. Kan automatisk justerer Security Group firewall rules baseret ejer og placering i application stack.

Software Defined Security programmer kan hele tiden overvåge clouden for policy violations. Kan automatisk fixe konfigurationer og sætter systemer i karantæne, eller identificerer ejere og anbefale ændringer.

Cloud Security principper

"Design for Failures" overvej flere availability zones osv. Nogle design-beslutninger er dine, ikke cloud-leverandørens ansvar.

Hvordan gemmes data på instancerne (instance er ustabile by-design). F.eks. bør en transaktionsdatabase ikke være på same host som database.
I Amazon skal data jævnligt flyttes til f.eks. S3.

Brug 'paranoid architecture', opdel services

Overvej kryptering når muligt, kryptering af data at rest

Cloud security

Pas på credentials på systemerne

Læg ikke top-level credentials ind i instancerne, hvis en instans bliver hacket bliver hele infrastrukturen kompromiteret

Læg ikke credentials i Source Code Repositories – eller andre steder der automatisk distribures til mange laptops.

Virtualisering og containers

Hvad er virtualisering ?

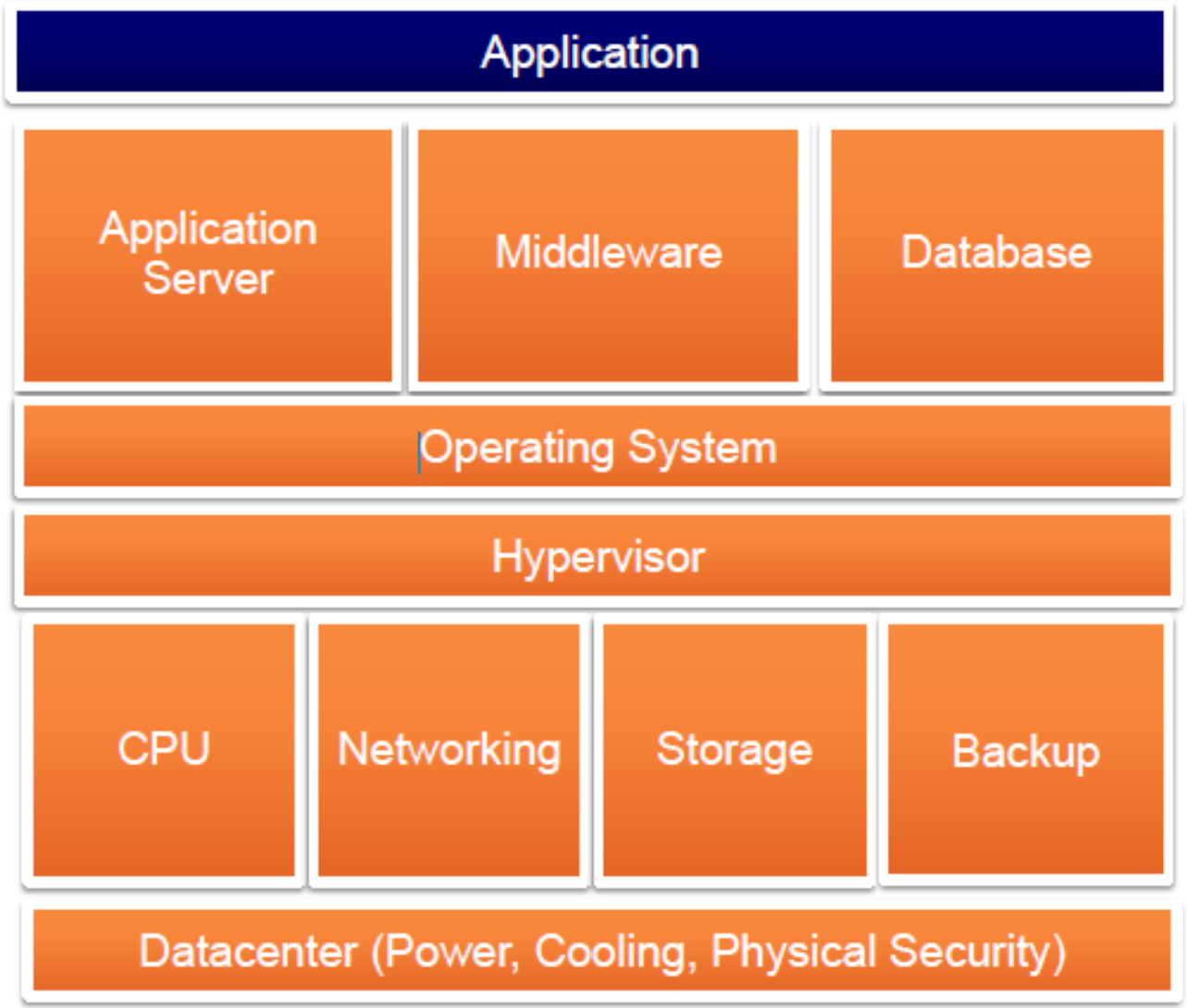
Hvad er virtualisering?

At få én fysisk enhed til at opføre sig som flere uafhængige enheder

Partitionere én fysisk server til flere ”virtuelle” servere, hvor hver ser ud til at køre som en dedikeret fysisk maskine. Hver server kan bootes uafhængigt af de andre.

Gæste operativ systemer/servere/storage

Hvad er virtualisering?



Gæst

Vært

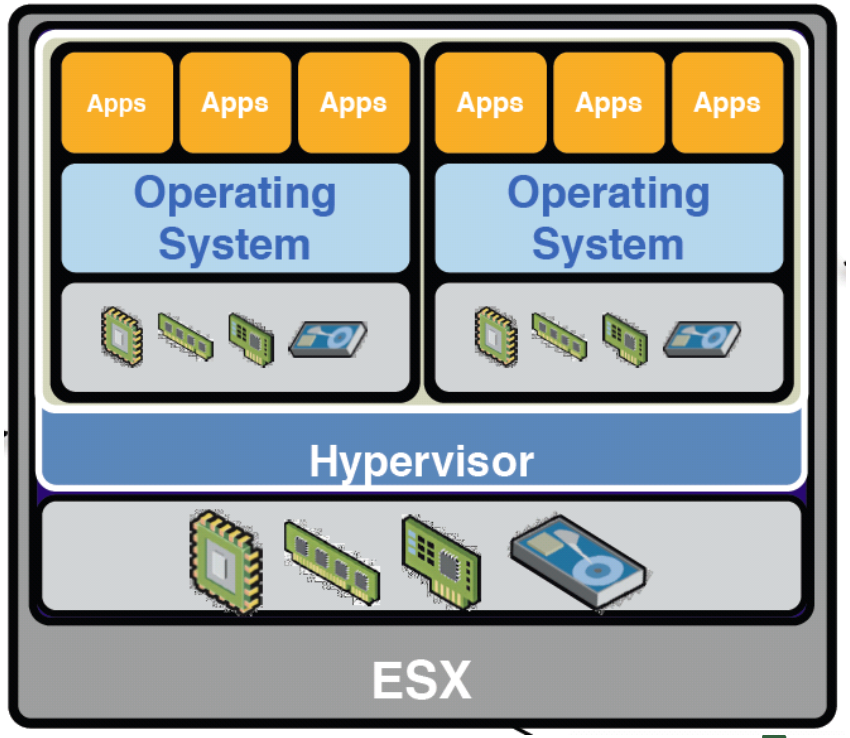
(Bare-metal eller Hosted)

Trusler imod virtualisering

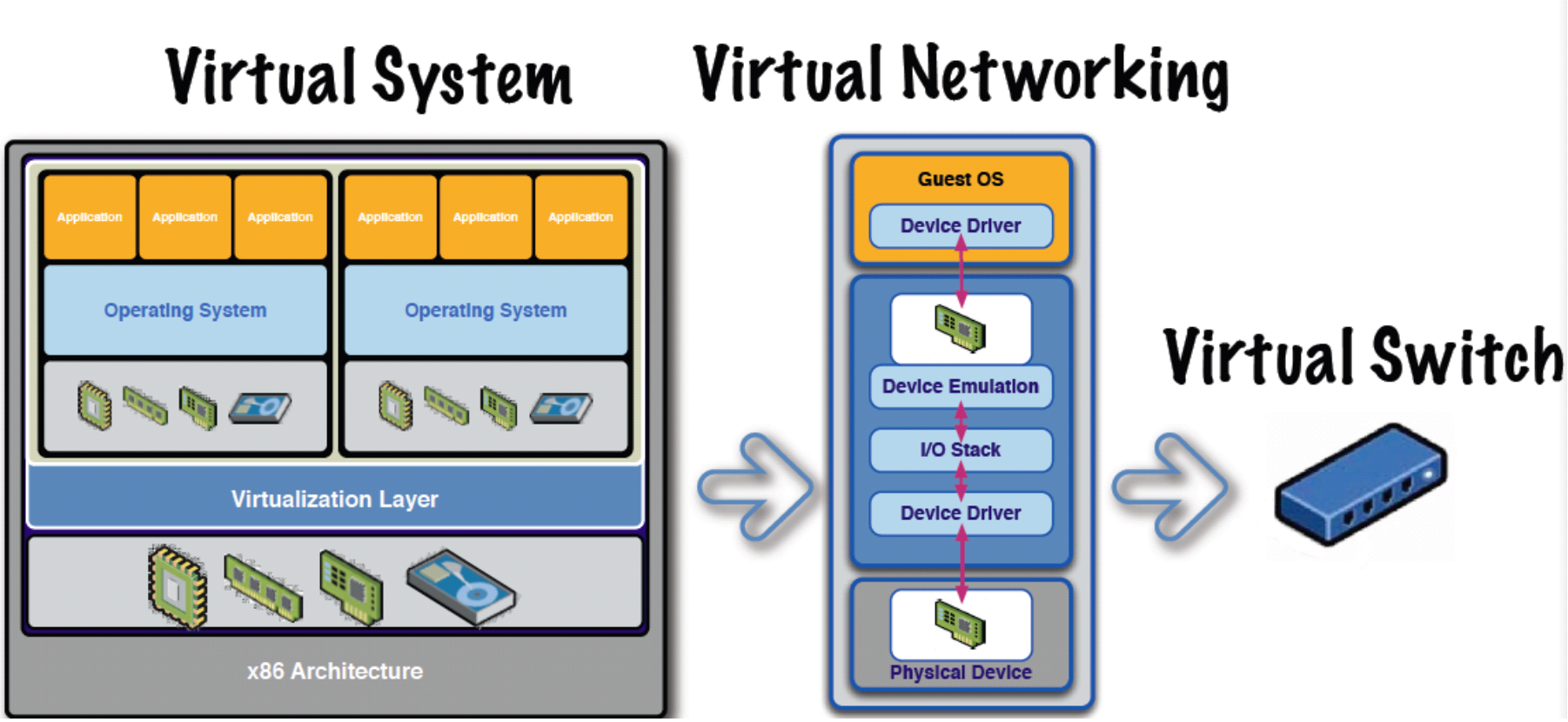
1. Guest to Self
2. Guest to Guest
3. Guest to Host/VMM/HW
4. External to Host/VMM/HW
5. External to Guest
6. Host/VMM to All...
7. Hardware to VMM

Administrationslaget…

Risikovurderingen



Trusler imod virtualisering



Trusler imod virtualisering

Sikkerhedslag kan flyttes til virtuliseringssoftwaren, f.eks. virusscanninger i hypervisoren

Udsætter hypervisor for potentielle risks

OS eller application layer: Host firewalls, AV, logning / log overvågning

Men - det påvirker performance og koster licenser, routning svært og beskytter ikke imod angreb inde fra de virtuelle miljøer

Virtualisering

Sikkerhedsproblemer opstår pga. fejlkonfiguration og dårligt design eller forkert implementering

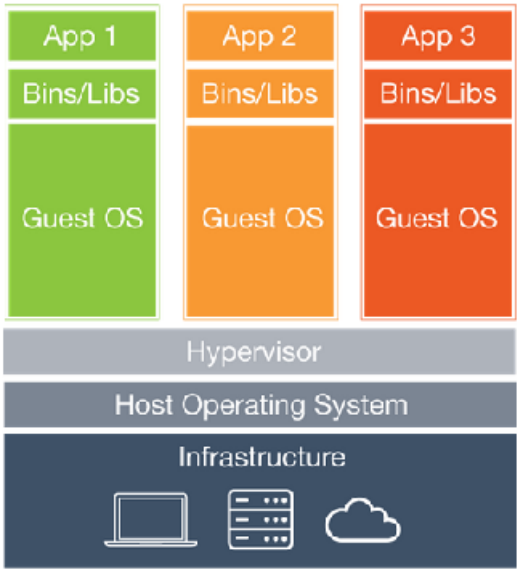
Alle leverandører har hærdningsvejledninger og best practice dokumentation

No free lunch

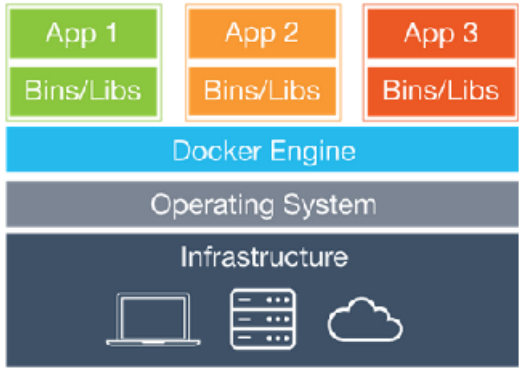
Containers and micro instances

Security isolation and application containment while improving resource efficiency over full virtual machines.

Linux containers provide segmentation via kernel namespaces, resource control via cgroups and are often secured through reduced root capabilities, Mandatory Access Control and user namespaces.



Virtual Machines



Containers

Containers and micro instances

Is the code running inside the container safe?

What has the container access to?

Who can it communicate with?

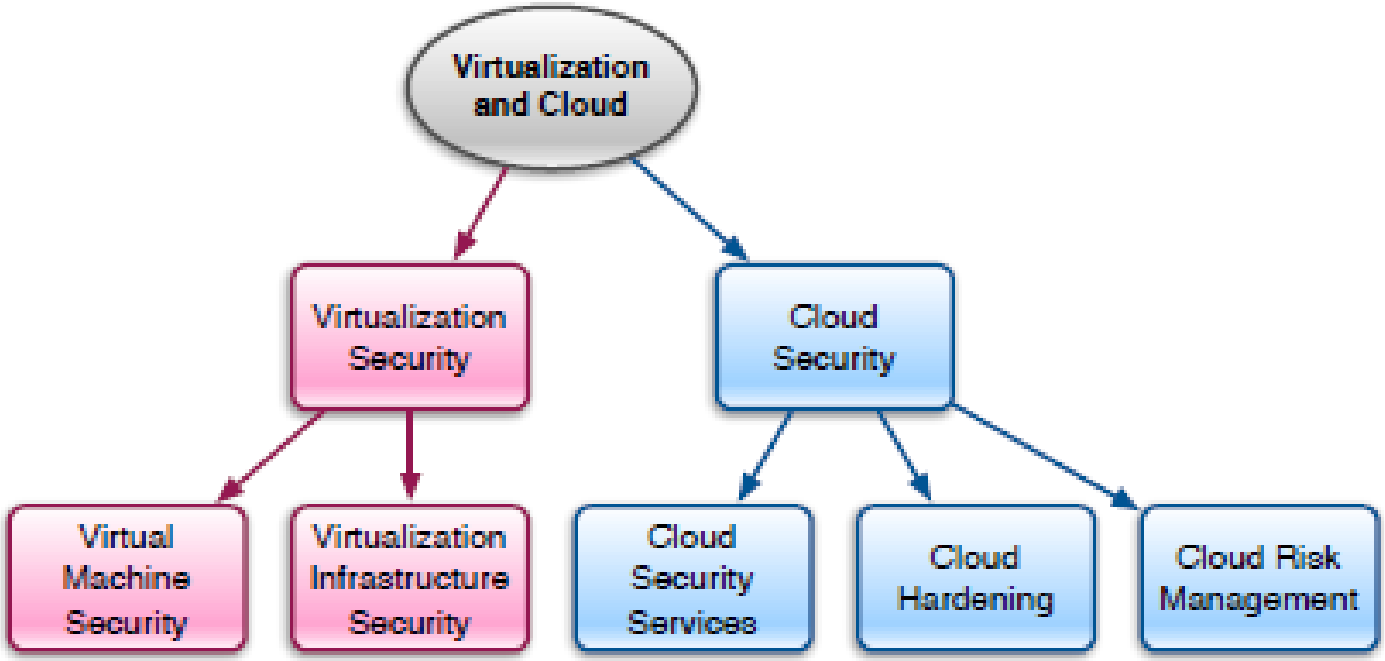
Where in the world is it running physically?

How is the container deployment and management ?

Containers collapses the security perimeter

No layer 3 security, app sec takes over

Virtualisering og cloud



Overlap, men ikke helt det samme

Pause

Serverless og Legoklodser

Serverless…?

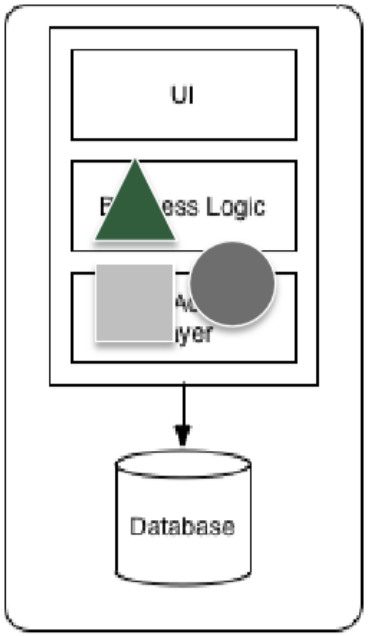
Ingen servere – ligesom der ikke er et køkken når du køber fastfood

Serverless…?

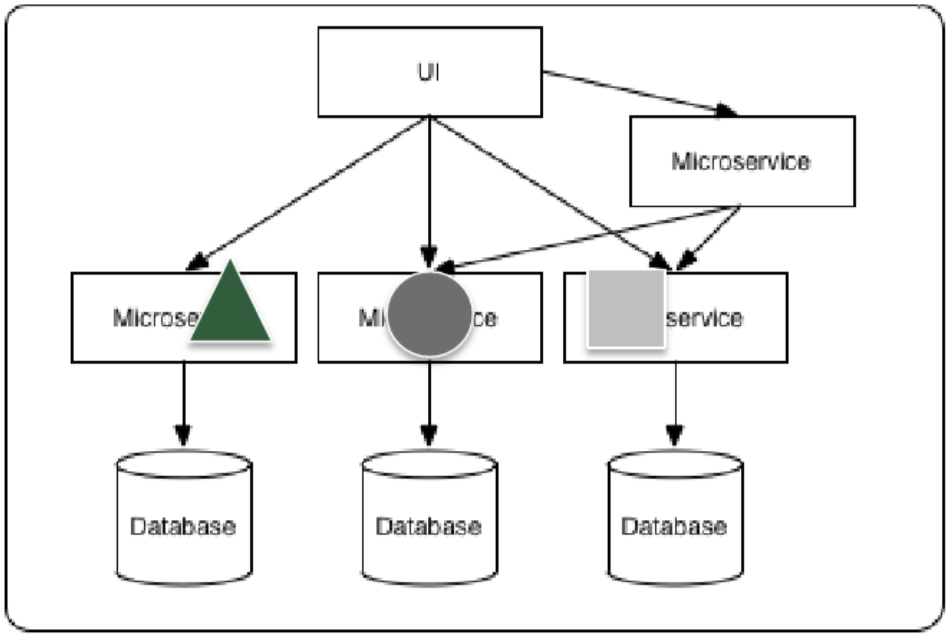
Eller – ligesom "Wireless" ikke har nogle kabler
(for dig, men der er mange, mange kabler bagved)

**Ingen servere – ligesom der ikke er et køkken
når du køber fastfood**

Begyndelsen – microservices…

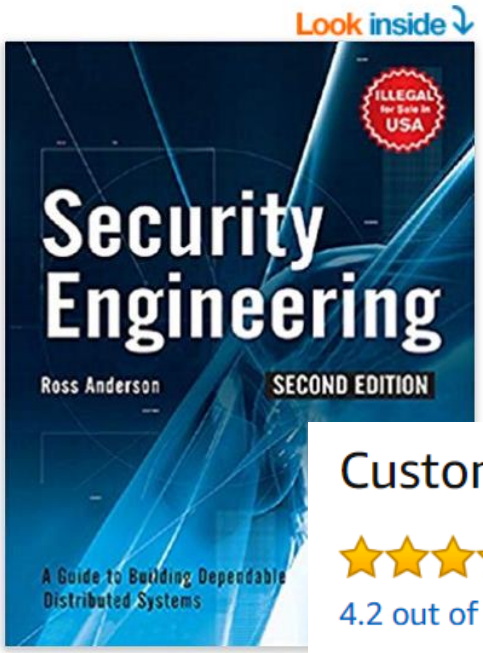


Monolithic architecture



Microservices architecture

Begyndelsen...



Frequently bought together

Total price: $43.30

Add all three to Cart

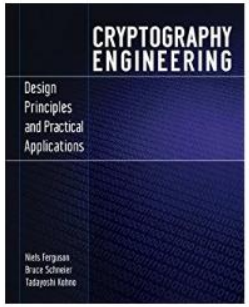
Add all three to List

These items are shipped from and sold by different sellers. Show details

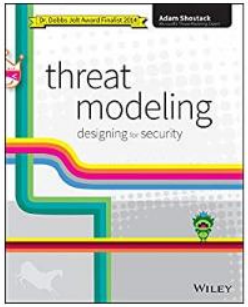
- **This item:** Security Engineering, 2ed by Ross J Anderson Paperback $20.31
- Secrets and Lies: Digital Security in a Networked World by Bruce Schneier Paperback $12.57
- Worm: The First Digital World War by Mark Bowden Paperback $10.42

Customers who bought this item also bought

ts and Lies: Digital
ity in a Networked
l
e Schneier
138
back
7 prime



Cryptography Engineering: Design Principles and Practical Applications
› Niels Ferguson
45
Paperback
$39.38 prime



Threat Modeling: Designing for Security
› Adam Shostack
33
Paperback
$35.00

Customer reviews

62

4.2 out of 5 stars

5 star	69%
4 star	15%
3 star	13%
2 star	0%
1 star	3%

See all 62 customer reviews ›

Serverless...?

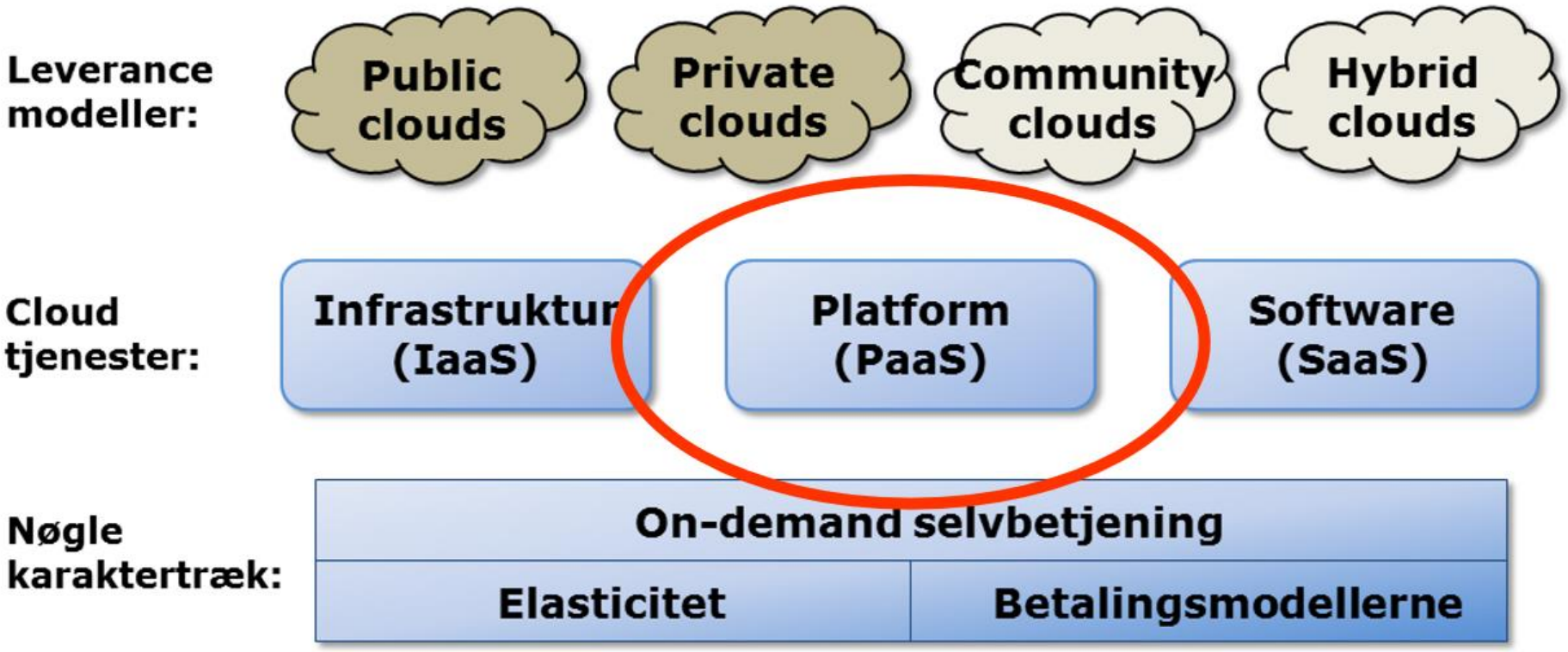
"Function-as-a-service" platforme

(AWS Lambda, Microsoft Azure Functions, Google Cloud Functions, Alibaba Cloud Functions, IBM Cloud Functions m.fl.)

Serverless er "event-driven"
Dvs udviklere skriver funktioner der reagerer på bestemte hændelser, en container starter indenfor 20-100 ms og lukker efter koden er kørt.
Der betales kun for de ms koden eksekverede.

Kunder kan ændre tilladte settings, men har ingen adgang underliggende hardware eller software

Serverless – ”PaaS”



Serverless ifht PaaS:

- PaaS er always on
- PaaS har ikke indbygget autoscaling
- Hvis en PaaS kan starte nye instancer på 20ms, der kører i et halvt sekund, så er det serverless

Serverless security 1

Ansvar for sikkerhed flytter fra netværk og infrastruktur til applikationen (og udviklerne)

- Ikke noget firewall team der ”lige kan fixe” manglende sikkerhed i applikationen
- Der er ingen perimeter – hver funktion er sin egen perimeter – hver funktion skal sikres!

Sikkerheden i Serverless er på platformsniveau, beskytter ikke application layer:

- SQL-injection, XSS, bad auth logic osv gælder stadig.

Test! Input validation over det hele, stol aldrig på input eller antag input er troværdigt osv.

Serverless security 2

Det hedder ikke ”data-less”: beskyt data

- Data er ikke længere opbevaret på serveren
- Kryptering
- Log og overvåg hvilke functions der tilgår hvilken data

Serverless security 3

Rigtige rettigheder og authorisation er stadig meget vigtigt

- Hvem kan kalde en funktion
- Hvem har adgang til selve funktionen
- Hvad kan en funktion gøre hvis den bliver kompromitteret (permissions outward)

Hver funktion bør kun gøre meget specifikke ting (brug meget granulære politikker)
Seperate credentials per function, begræns hvad hver credential kan gøre

Pas på implicit trust mellem microservices/functions, vil ofte være udviklet af forskellige teams (og ofte i forskellige sprog)

Serverless security 4

Begrænsede rettigheder (least priviledge)
- Det skal sikres, at funktioner kun har de nødvendige rettigheder til at kunne udføre sine opgaver (ingen ”*”)

```
- Effect: Allow
  Action:
    - 'dynamodb:*'
  Resource:
    - 'arn:aws:dynamodb:us-east-1:**********:table/TABLE_NAME'
```

```
- Effect: Allow
  Action:
    - dynamodb:PutItem
  Resource: 'arn:aws:dynamodb:us-east-1:**********:table/TABLE_NAME'
```


Serverless security 5

Stort brug af 3.part tjenester - forstå hvem du stoler på og hvor meget

- Verify, verify, verify
- Inventory list over software pakker og andre afhængigheder, scanninger,
  fjern unødvendige dependencies, opdater…

- Overvej dataflow: hvor er min data, er det tilstrækkeligt sikret, overvej kontroller for hvert set af data (eller i hvert fald for hver kategori af data)

Muligheder for forbedringer af sikkerheden

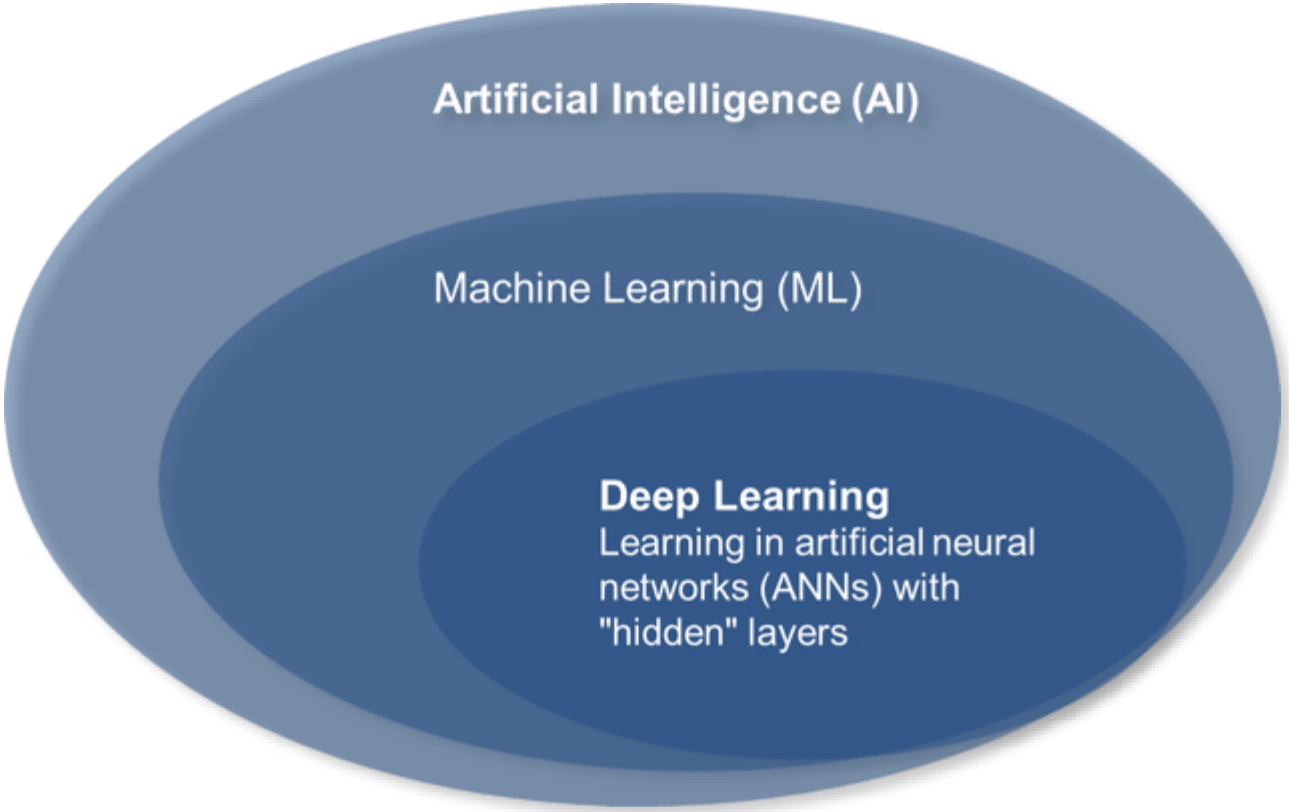
- Altid krypteret trafik (hvis i gør det rigtigt)
- Brug 2FA - Certikater til service-autentifikation
- Meget mindre attack-surface (hvis du har valgt en god cloud-leverandør) – f.eks. ingen portscans af functions
- Fjerner adgangsveje for angriber
- Service segragation
- Selv med komponenter, der ikke er serverless kan attack-chain ødelægges
- Software-defined security – automatisering og integrering af mange sikkerhedsopgaver
- Event driven security – automatiske handlinger baseret på aktiviteter

Cloud computing

- Forstå *den cloud i overvejer*, ellers kan man ikke sikre den
- Risiko analyse og risk management – som altid
- Vælg en sikkerhedsarkitektur
- Sund fornuft – cloud er ikke magi, det er it-systemer der bruger strøm

AI security

Hvad er ”AI”?


Artificial Intelligence (AI)
Machine Learning (ML)
Deep Learning
Learning in artificial neural networks (ANNs) with "hidden" layers

AI - risici og sårbarheder

Eksisterende risici

Ændrede kendte, eksisterende risici

Helt nye og ukendte risici

AI ændrer ikke alting sikkerhedsmæssigt

Hvilke komponenter kan indgå i AI-løsninger

Træningsdata

Algoritmer og modeller

Netværk/internet

Hardware/software

Fysiske komponenter

Hvilke trusler kan en AI-løsninger være udsat for

Hvem er angriberne?
Hvordan kan det gå galt?

Nogen forsøger at stjæle vores model eller vores data, indbygget diskriminering i model, angriber manipulerer træningsdata…

Sikkerhedsproblemer i AI opstår grundlæggende opstå som
1) følge af fejl og
2) som følge af bevidste, direkte angreb.

Lige nu er fejl hovedårsagen til sikkerhedsproblemer

Hvilke trusler kan en AI-løsninger være udsat for

AI sikkerhed
AI som angrebsmål

Angreb imod AI:
Adversarial AI
Adversarial inputs to ML/AI
Inference attacks
Resilience attacks (Denial of Service etc.)
Fysiske angreb
Osv, osv

Tyveri af AI:
Formål: stjæle intellectual property - eller at lave en kopi/substitute model for at udvikle angreb imod oprindelige system.

Stjæler data eller træningsdata.
Stjæler algoritmer

Fejl:
Data:
Fejl i data
Bias/social slagside pga benyttede træningsdata
Model:
ML model brugt forkert
Almidelige fejl ved deploying, designing and training
Andre eksempler:
GDPR issues
Privacy

Aktiv angriber

Opstår som følge af fejl

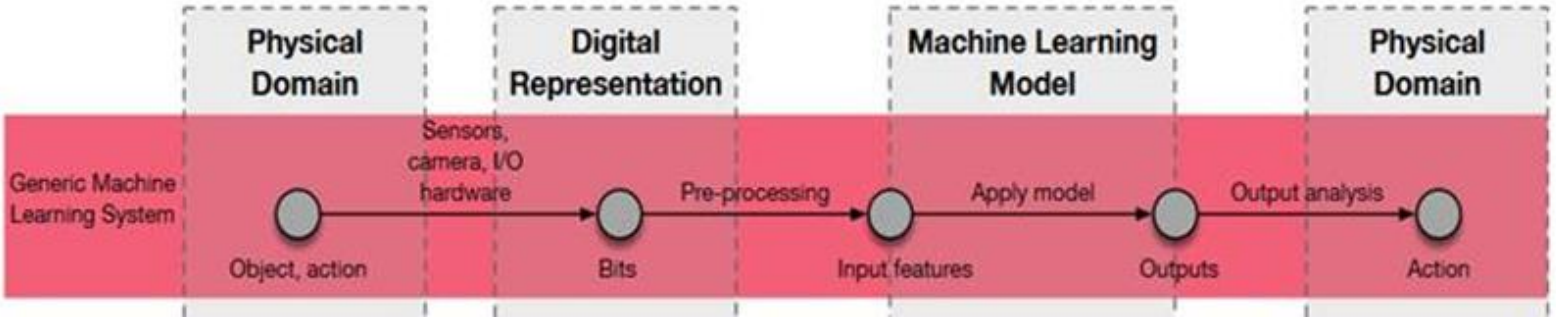
Metode til at identificere mulige angreb og sårbarheder

For at kunne vurdere sikkerheden i AI må man forstå hvor sårbarhederne kan opstå - AI "angrebsoverfladen" kan bruges til at identificere komponeterne

Angreb kan ske imod de underliggende systemer
(AI er hardware og software)
IT-sikkerhed er helt fundamental - grundkrav for brug af AI
Hardware sikkerhed
Cloud sikkerhed
Sikkerhed i algoritmer og modeller
Hvad laver algoritmen/modellen egentlig, hvordan er de sikret, fall-back etc, etc.
Forskellen på "Bevidste, direkte angreb" og "Accidential problems"
AI supply chain sikkerhed
Garbage in - garbage out: hvor kommer træningsdata fra. Kan en angriber påvirke systemet, f.eks. ved at sende mislabled data eller tvinge en Reinforcement Learning (RL) algoritme i en bestemt retning osv.
Både fysiske og digitale angreb
Angreb kan ske imod data, algoritmer og modeller, men også imod f.eks. vejskilte eller kameraer

Metode til at identificere mulige angreb og sårbarheder

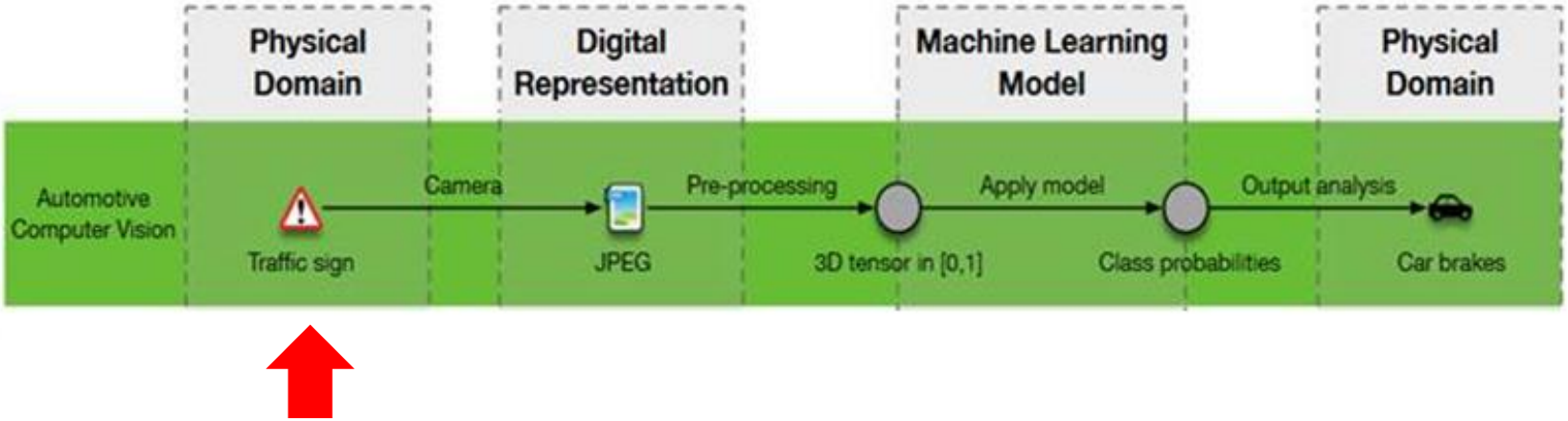
For at kunne vurdere sikkerheden i AI må man forstå hvor sårbarhederne kan opstå - AI "angrebsoverfladen" kan bruges til at identificere komponeterne



SoK: Towards the Science of Security and Privacy in Machine Learning (Papernot et.al) - https://arxiv.org/pdf/1611.03814.pdf

Vurder attack-surface i den enkelte løsning – f.eks. opstår faren for "Poisoning/Enchanting" angreb primært når AI-løsningen benytter Reinforcement Learning, eller angriber kan sende angrebs-data til AI-løsningen (digitalt eller fysisk).

Metode til at identificere mulige angreb og sårbarheder

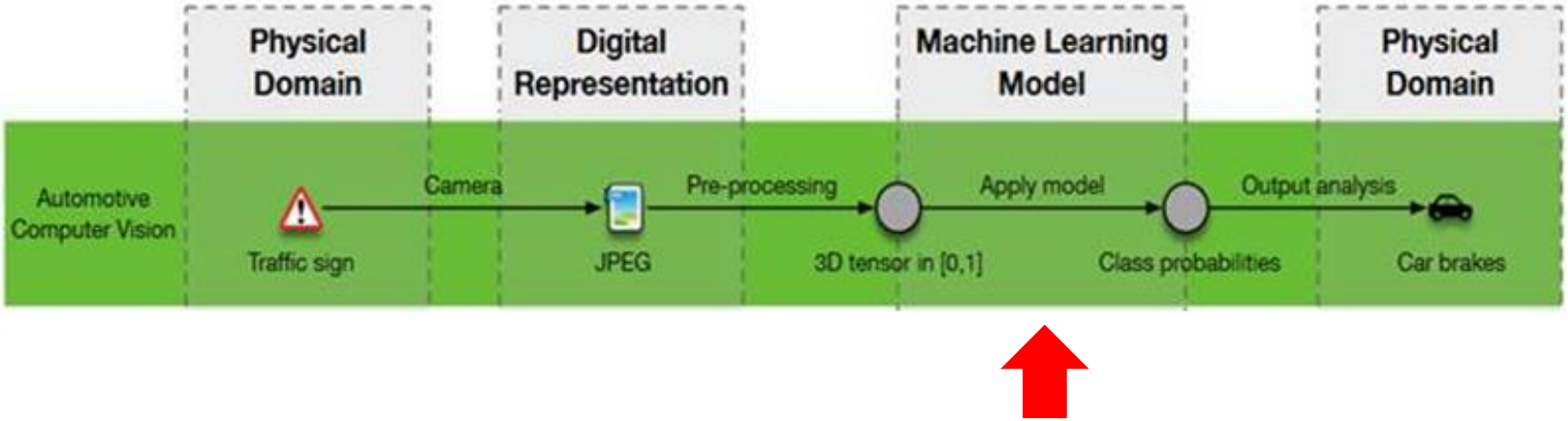


Eksempel 1: selvkørende bil

1. Angreb imod et selvkørende køretøjs even til at genkende trafik-skite - fysisk angreb imod f.eks. trafikskilte

Overvej mulige konsekvenser for individer, virksomheder og for samfundet som relevant for jeres risikovurdering

Metode til at identificere mulige angreb og sårbarheder

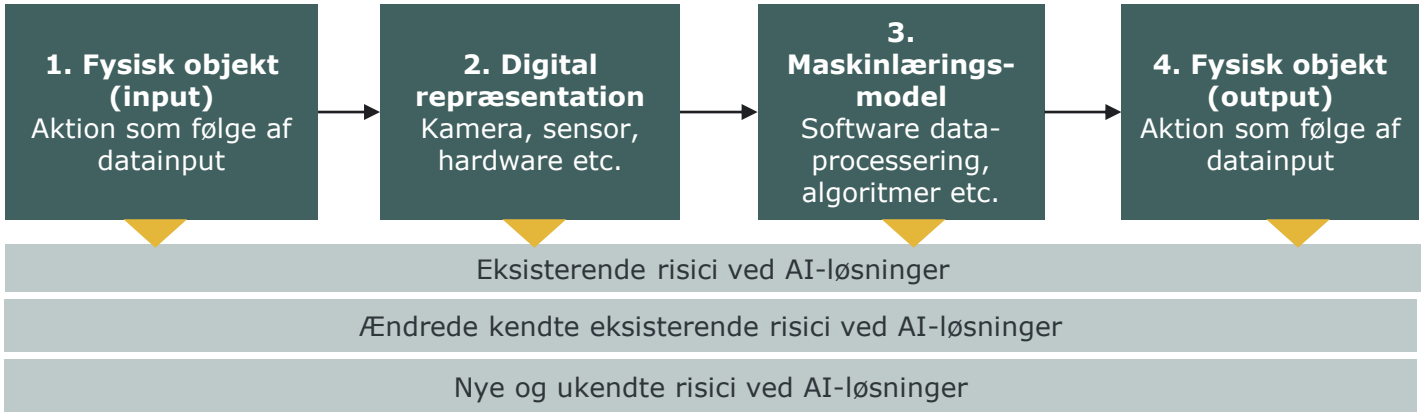


Eksempel 2: selvkørende bil

1. Angreb imod et selvkørende køretøjs even til at genkende trafik-skite - poisoning attack imod input data

Overvej mulige konsekvenser for individer, virksomheder og samfundet som relevant

AI risici og sårbarheder



AI risici og konsekvenskategorier

AI sårbarheder kan have digitale, fysiske og/eller politiske konsekvenser:

1) AI er software og hardware, så der er potentielle IT/Cyber-sikkerhedskonsekvenser – (fortrolighed, integritet, tilgængelighed osv.)
2) Fysisk sikkerhed (f.eks. ifht droner, IoT og selvkørende biler)
3) Samfundsmæssig/politisk sikkerhed (fake news, tillid osv)

Konsekvenser i tre hovedkategorier:

1) Konsekvenser for personen [privacy, reputation, loss of intellectual property, physical harm, …]
2) Konsekvenser for virksomheden [tab af omsætning, udgifter, reputation, loss of intellectual property, bias…]
3) Konsekvenser for samfundet [fake news, manipulation of online information, financial harm, trust, …]

Første del af risikovurderingen

Hvor?	Fysiske angreb	Angreb imod IT-systemer	Model/algoritme
Data indsamlings fasen	• **Angreb imod sensorer** for at påvirke AI-løsning (f.eks. kameraer og IoT devices) • **Angreb imod omgivelser** for at påvirke AI-løsning (f.eks. vejskilte)	**Angreb imod data repositories** (f.eks. datasets)	
Træningsfasen			• **Injection** inserting adversarial inputs into existing training data • **Modification** Altering training data directly • **Learning algorithm tampering** Logic corruption

Konsekvens -> ”bil kører over for rødt lys” eller ”løn udstedes uberettiget”
og **håndtering**(- Security Management forelæsningen)

Hardware hacking

Hvad kan man gøre med fysisk adgang til hardware?

(kort introduktion)

Fysisk adgang til hardware

Hardware er selvfølgelig grundlaget for software, algoritmer og kommunikation.

Hardware skal sikre, at kun den autentificerede bruger har adgang til processoren.

Men:
Hardware design har normalt ikke sikkerhed som et nøgle designmål.

Hardware bliver ofte det svage led i sikre systemer.

Fysisk sikkerhed er mange forskellige ting

HOWTO defeat a sliding chain lock with a rubber band:
http://www.youtube.com/watch?v=7INIRLe7x0Y

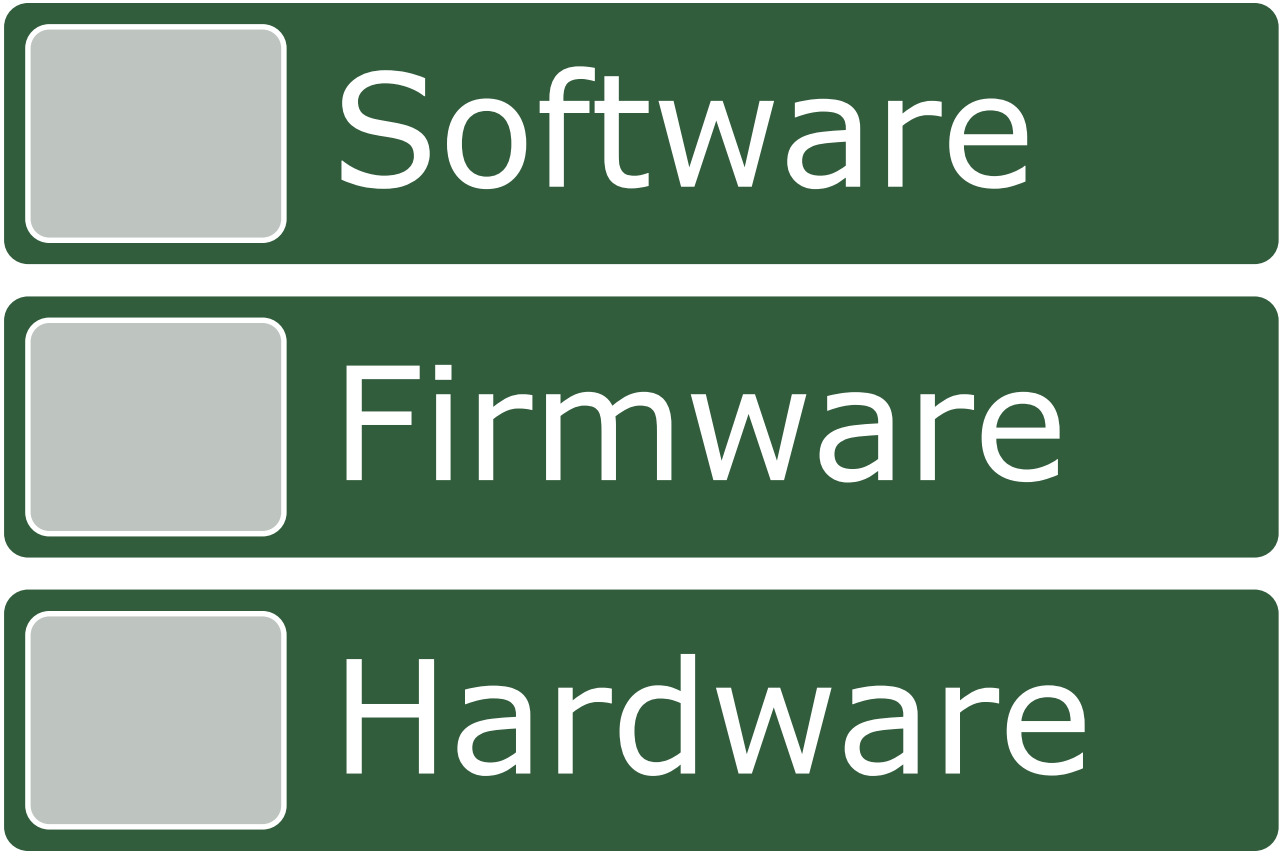
Locked suitcase:
https://www.youtube.com/watch?v=G5mvvZl6pLI

Opening a computer lock cable:
http://www.youtube.com/watch?v=TPDgX9P8xLQ

Cykellås:
http://www.youtube.com/watch?v=_2vLtpVPqhI

Bypassing security measures

Tre niveauer



Fysisk sikkerhed er mange forskellige ting

Evil Maid attacks

Towards the cloud – and beyond

Many To One

Mange brugere
En enkeltstående
central server

I forgårs

One To One

En bruger
En computer

I går

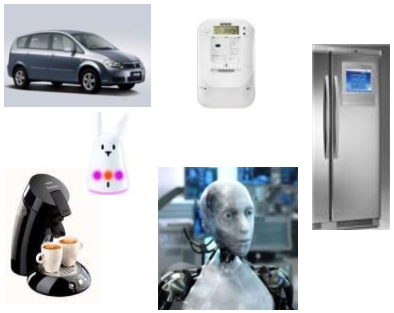
One To Many

En bruger
Mange medier

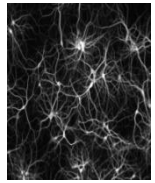
I dag

Machine To Machine

Many To Many



I morgen



Neuro-
Nano-
technologier

I over-morgen


Retweeted by the grugq
Matt Haughey @mathowie · 13 hrs
What am I doing? Oh just waiting for my garage door opener to join WiFi so I can get back into my house #2014problems
Verizon 9:51 AM 62%
Places
PLACE
Garage Door Opener
No Response
MyQ Server not responding. Please try again later.
OK

Why defend hardware?

Kan enheder klones? (økonomisk tab pga salg af kopi-enheder, risiko for negative omtale fordi folk tror enhederne er ægte osv)

Kan softwaren stjæles?
Kan hardware design stjæles?
Kan angriber ændre funktionalitet?

Hvor stort budget har angriberen, hvor motiverede er de, kan angriber ødelægge enheden?

Rejsekort – bilnøgler - militære enheder
Supply chain verification

People will have physical access to the hardware

Smart cards, phones, cars, RFID, TV etc., etc…

Software

Firmware updates

RAM dump (keys, credit card info etc)

So what can you do to test or assess hardware?

Fysisk adgang til hardware

1. Design walk-through:
High level impression (messy, professional, hidden)

ChipWorks, iFixIt etc. take apart many types of hardware
Can be good starting points, otherwise time for desoldering components - and Google

2. Find interaction points - explore with a multimeter to catalogue hardware interaction points and potential debug interfaces.

Fysisk adgang til hardware

Mass produced hardware needs to be tested prior to deployment.

Interesting or problematic areas of the board have testing points exposed on the outer layers so external testing machines quickly can validate them on the production line.

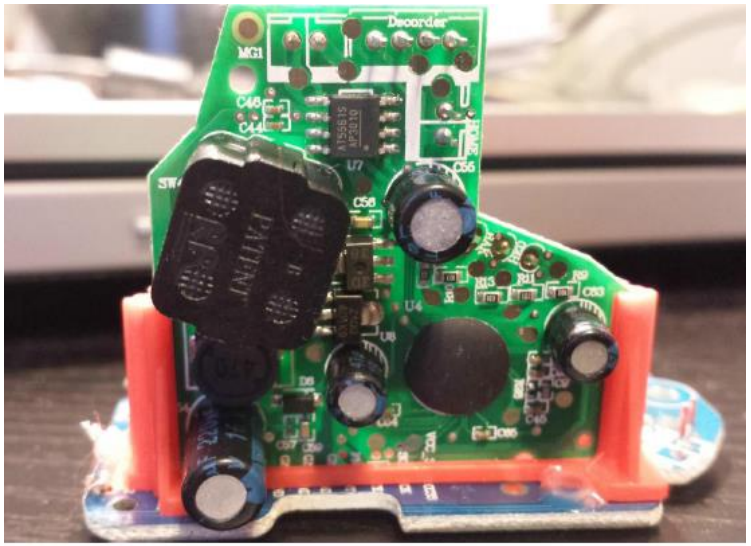
Hardware designers tend to expose debug functionality with these interaction points to allow for firmware and OS flashing post production.

Fysisk adgang til hardware

Tracing all the pins and attempting to recreate the full schematic.
Then acquire spec sheets for every piece of silicon

Start looking for **debug or flashing capabilities**.
The main focus of this part of a hardware analysis is to plan an **attack to grab the resident firmware (or ram)**.

Also explore the USB side of the hardware and look at an available driver/os/kernel

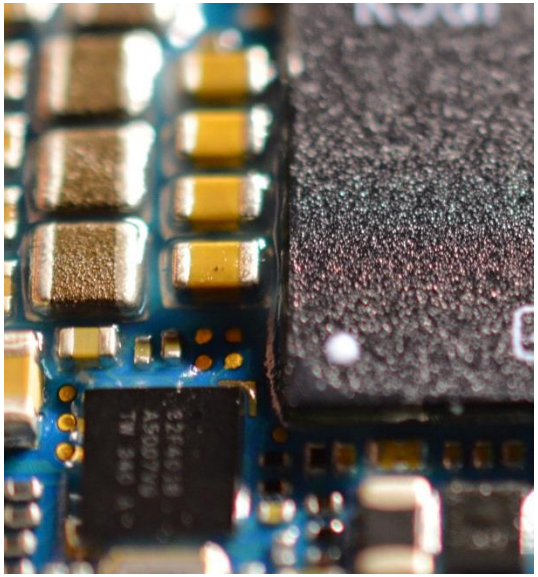


Fysisk adgang til hardware

What we really care about is:

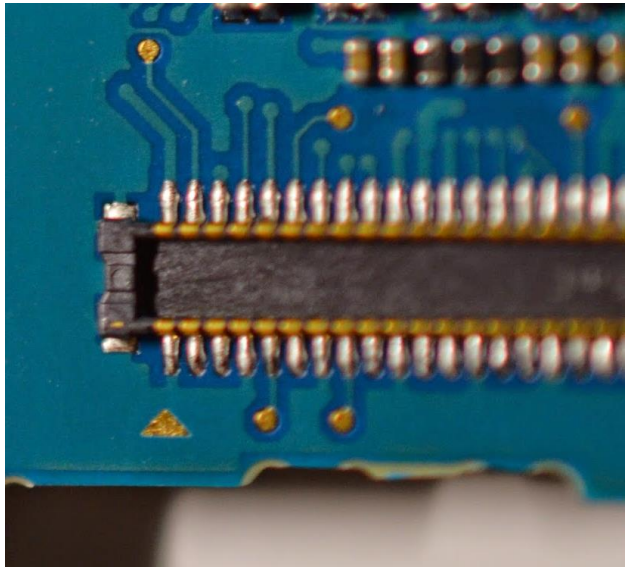
- What components are being used
- How was the device built
  Did the designers leave any debugging mechanisms exposed or active during production
- Are there any weak parts of the design that look easily exploitable

Fysisk adgang til hardware



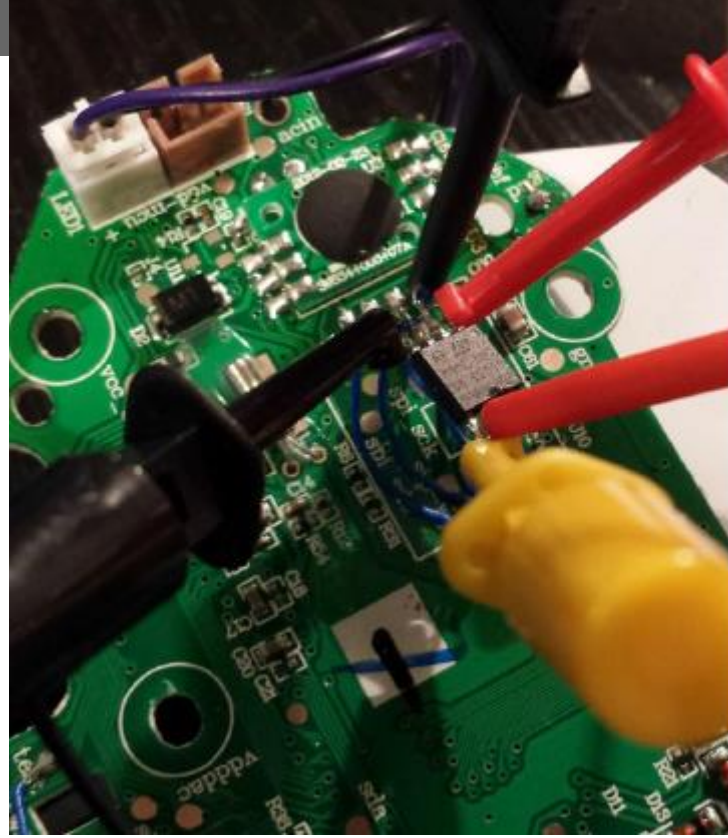
The device must be loaded with software and most vendors protect that functionality with a series of hardware flags controlled by resident voltages. Tracing the pads with a multimeter to see where the missing discrete components would effect, and what circuit they could complete if bridged.

Fysisk adgang til hardware



Ribbon cable seat. The pinouts can be latched with a logic analyzer to watch all the data pass over the cable is possible - much easier than tapping the cables directly.

Fysisk adgang til hardware



Nintendo Wii
Tweezer hack –> private keys

Buffer overflow in save system of Legend of Zelda: Twilight Princess:

Using a modified save file containing a name for Link's horse long enough to cause a buffer overflow pointing to a memory address which contained the loader code.

APP

Side-channel attacks

What else can I do with the device?

Side-channel attacks

Can successfully reveal the secret cryptographic keys stored in secure systems

These attacks include:

- power analysis,
- timing attacks, and
- electromagnetic attacks

Fysisk adgang til hardware

Extracting the Private Key from a TREZOR with a 70 $ Oscilloscope

http://johoe.mooo.com/trezor-power-analysis

Hardware hacking

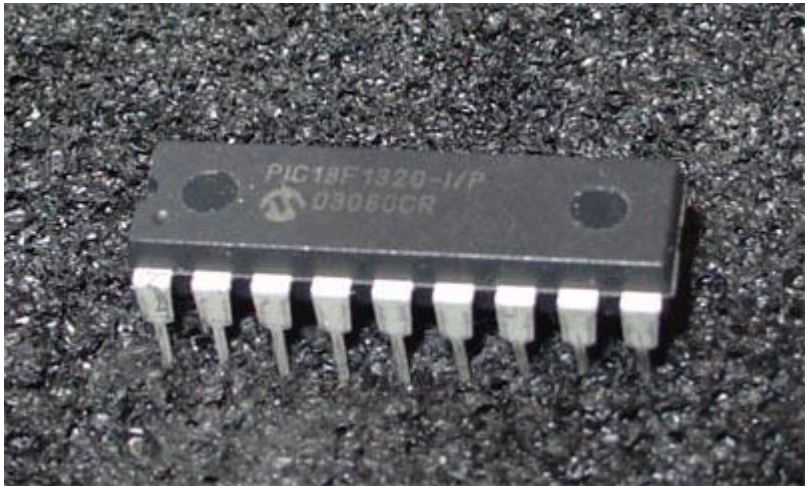
Physically attacks against the chip to extract the key

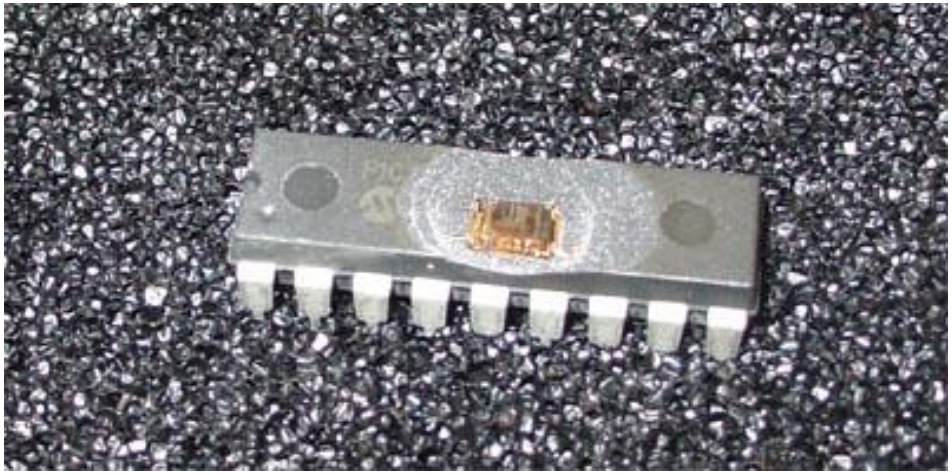
30.000 dollars for "real" microskope, but still not unrealistic

A chip can get cappet for less than 80 dollars on the internet + 600 dollars for an adequate microskope

Decapping chips with acid

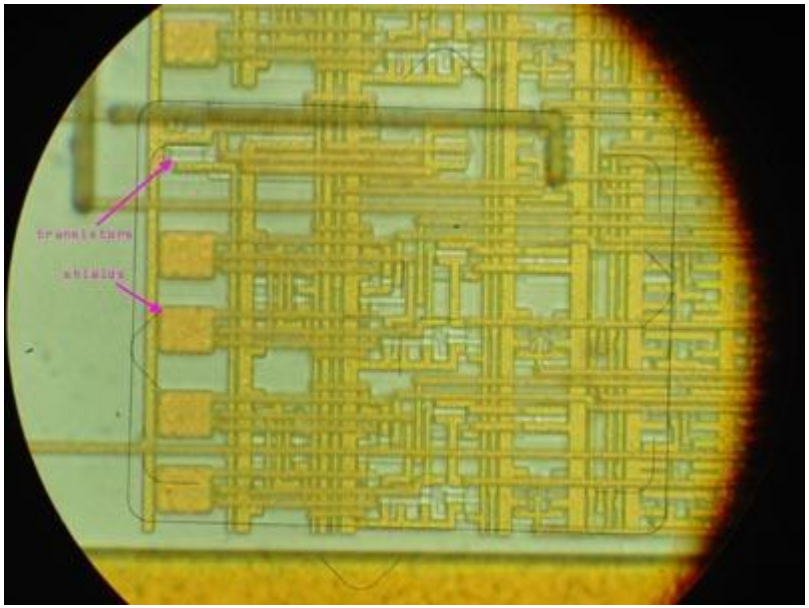
Microskope
Probe when the chip has power

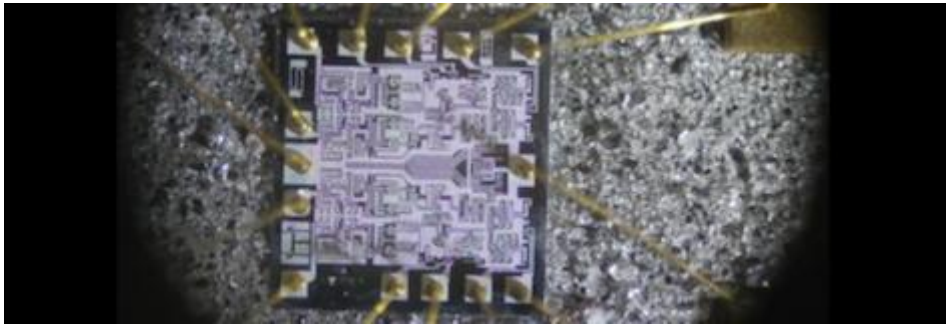




Decapping chips with acid

Microskope
Probe when the chip has power

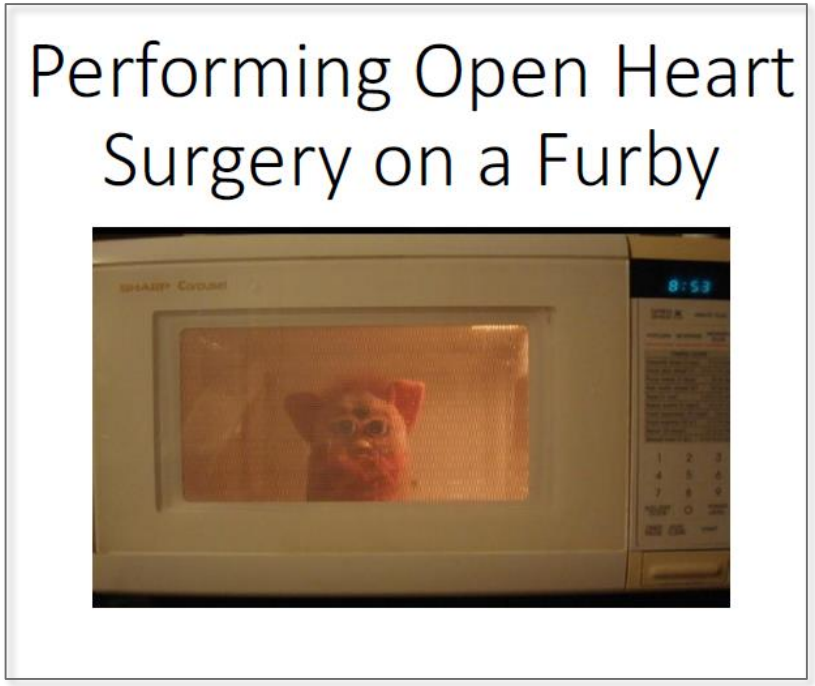




Decapping chips with acid

Microskope
Probe when the chip has power

Hardware hacking – a couple of starting points



http://recon.cx/2014/slides/Performing%20Open%20Heart%20Surgery%20on%20a%20Furby%20Recon%202014.pdf

http://www.siliconpr0n.org/

IoT Security

What is "The Internet of Things" (IoT)

IoT is a term that refers to the expanding interconnection of smart devices, ranging from appliances to tiny sensors

- A dominant theme is the embedding of short-range mobile transceivers into a wide array of gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves
- The Internet supports the interconnectivity usually through cloud systems

The objects deliver sensor information, act on their environment, and in some cases modify themselves, to create overall management of a larger system

The IoT is primarily driven by deeply embedded devices

- These devices are low-bandwidth, low-repetition data capture, and low-bandwidth data-usage appliances that communicate with each other and provide data via user interfaces
- Embedded appliances, such as high-resolution video security cameras, video VoIP phones, and a handful of others, require high-bandwidth streaming capabilities

What is IoT/Internet of Things?

Millions of devices
Communication and protocols - NB-IoT, LoRa, Sigfox, etc. - or Zigbee, RFID, WiFi

Simple, cheap: sensors, meters (smart parking, pet-tracking, temperature, humidity, intelligent meters, asset tracking etc.)

Fast, expensive: Smart cars, smart homes/consumer electronics, CCTV/cameras, healthcare, TV etc.

Smart city, Industry 4.0, Smart Agriculture

Cows/pigs/bees, bicycles, fire alarms, smart bin, street light, environment/pollution/noise, etc., etc.

Is IoT/Internet of Things secure?

Threat modeling – the 5 questions

1. What do you want to protect?
   Assets
2. Who do you want to protect it from?
   Adversaries and threats
3. How likely is it that you will need to protect it?
   Probability
4. How bad are the consequences if you fail?
   Risk
5. How much trouble are you willing to go through in order to try to prevent those?
   Value

The Security Management lecture in October

What is IoT/Internet of Things?

1. What do you want to protect?
   Assets

Describe the specific solution

Consider your viewpoint:
- User
- Vendor/developer
- Customer
- State/global
- …

What is IoT/Internet of Things?

1. What do you want to protect?
   Assets

You are responsible for security in a Danish company. A number of burglaries have taken place at night at other companies, and management want to improve physical security on all your locations.

Currently a guard company checks (almost) every night if doors and windows are closed.

Your suggested solution will use 2 IoT-solutions:

What is IoT/Internet of Things?

1. What do you want to protect?
   Assets

1) Small sensors on all windows and all doors will check every hour if closed. If open an alarm is sent from device, through company network, to the monitoring system (cloud-based).

2) 4K video cameras are placed outside the building and inside in every office covering all rooms, including kitchen and toilets.
   Video-feed is streamed over the internet to a monitoring system, AI will automatically send an alarm if suspicious behavior is detected.

What is IoT/Internet of Things?

1. What do you want to protect?
   Assets

If alarm is received video can be watched and/or a guard can be sent on site. Police can be called, if necessary.

100 devices

10.000 devices

IoT/Internet of Things - Threats?

1. What do you want to protect?
   Assets

10.100 devices

Network → Internet → IoT Cloud Platform

What is IoT/Internet of Things?

2. Who do you want to protect it from?
Adversaries and threats

- Battery or power… Computer or simple chip…
- Low-cost devices cannot support standard security technologies like virus protection or anti-malware
- Physical access to devices, many devices

Network → Internet → IoT Cloud Platform

IoT/Internet of Things - Threats?

- Devices on company network - or directly on Internet?
- Large attack-surface: protocols, devices, platforms etc.
- Privacy
- Upgrades
- IoT-provider security

Devices → Network → Internet → IoT Platform

CIA

Confidentiality
Integrity
Availability

Fortrolighed – Integritet - Tilgængelighed

IoT/Internet of Things - Threats?

Encryption (transport and local)
Authentication

Attacks against cloud platform and services

Confidentiality

IoT/Internet of Things - Threats?

IoT insecurity: Casino hacked through smart thermometer

Hackers stole a casino's high-roller database through a thermometer in the lobby fish tank

OSCAR WILLIAMS-GRUT | APR 15, 2018, 12.42 PM

IoT/Internet of Things - Threats?

Trust the sensors/data?

IoT/Internet of Things - Threats?

DoS/DDoS risk?

Availability risks?

IoT/Internet of Things - Threats?

Computer og strøm

- PKI
- VPN
- Security upgrades
- Anti-virus/anti-DoS

Chip og batteri

- Lightweight authentication/PSK
- Lighweight encryption (only important data)

Spørgsmål