



Denne forelesningsøkten vil bli tatt opp og lagt ut i emnet i etterkant.

Hvis du ikke vil være med på opptaket:

 Start Video	La være å delta med webkameraet ditt.
 Unmute	La være å delta med mikrofonen din.
To: Marianne Sundby (Privately) Type message here...	Still spørsmål i Chat i stedet for som lyd. Hvis du ønsker kan spørsmålet også sendes privat til foreleser.



Høyskolen
Kristiania

TK2100: Informasjonssikkerhet

10. forelesning

Pensum:

Goodrich & Tamassia (2011),
490-502, s 509-517

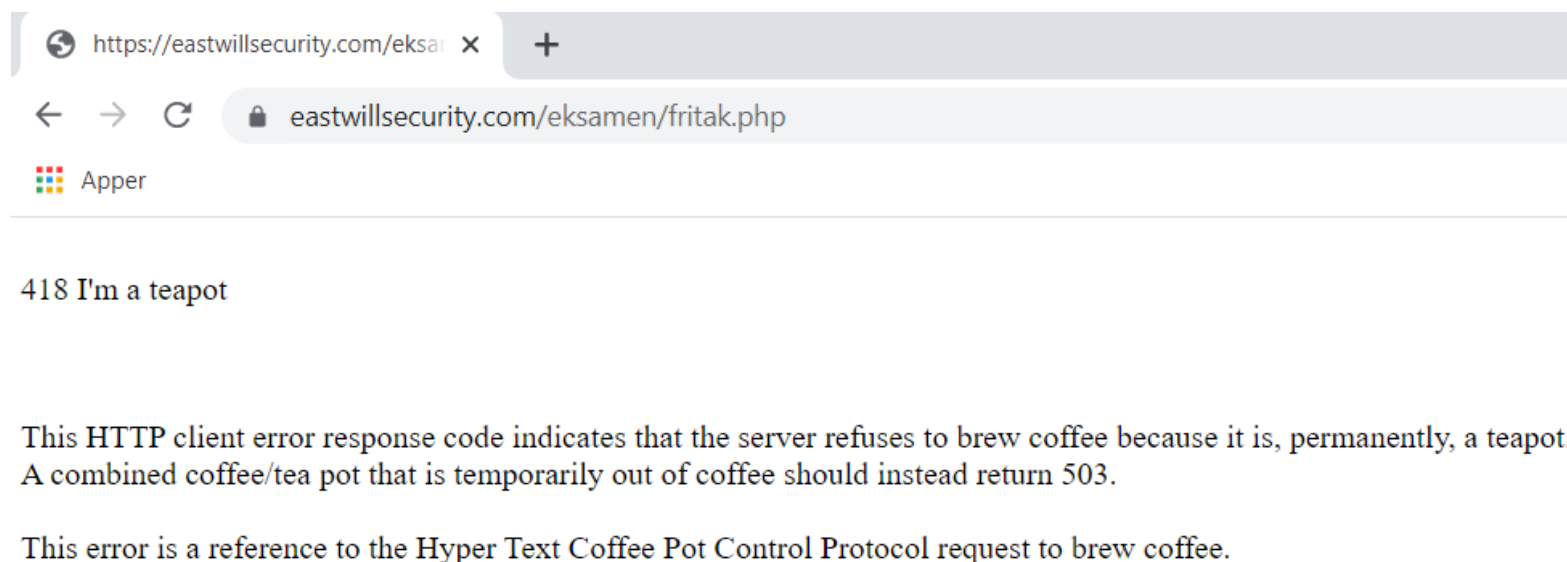
G&T (2014), s. 458-470, 477-88

ARBEIDSKRAV

- Husk innlevering av arbeidskrav på torsdag!
- Frist torsdag 7. april klokken 23.59

Årets aprilspøk ☺

- Kunngjøringen som ble lagt ut 1. april var selvsagt en april-spøk ☺
- For de som trykket på linken så fikk de opp en referanse til en annen april-spøk når web serveren returnerte en 418 feilmelding



- Og kan samtidig minne om hva vi har lært om å trykke på «phishing linker», totalt 284 studenter klikket på linken i løpet av dagen...

RFC 9225 (1. april 2022)

- <https://www.rfc-editor.org/rfc/rfc9225.html>
- En ny internasjonal standard for programmerere ble sluppet på fredag, jeg trekker frem to punkter som jeg synes oppsummerer standarden:
 1. Authors **MUST NOT** implement bugs.
 2. If bugs are introduced in code, they **MUST** be clearly documented.

I dag

- Opphavsrett, patenter
- DRM
- Epost og spam
- Internet of Things

Immaterielle rettigheter og DRM

- Tanker, ideer og teorier tilhører ingen
- Formuleringer og utforminger kan derimot tilhøre noen
 - I et (juridisk) begrenset tidsrom

Die Gedanken sind frei, wer kann sie erraten,
sie fliegen vorbei wie nächtliche Schatten.
Kein Mensch kann sie wissen, kein Jäger erschießen
mit Pulver und Blei: Die Gedanken sind frei!

Immaterielle rettigheter

- **Immaterielle rettigheter** er felles-betegnelsen på eiendom som ikke er knyttet til enkeltgjenstander
 - **Opphavsrett** til åndsverk
 - Bøker, dikt, sanger, bilder, foto, formelsamling, **dataprogram**, ...
 - **Patenter** på oppfinnelser
 - Produkter, metoder,
 - **Varemerker**
 - F.eks. firma-logo, navn,
 - **Design**
 - Stoler, tannbørster, **knapper**, **websider**



Verdens mest verdifulle varemerker

- Merkevarer i seg selv har en verdi, her Forbes 2019 listen:



#1 Apple



#2 Google



#3 Microsoft



#4 Amazon



#5 Facebook



#6 Coca-Cola



#7 Samsung



#8 Disney



#9 Toyota



#10 McDonald's

- Gir **enerett** til **kommersiell** utnyttelse av en **oppfinnelse** for et begrenset **tidsrom** (20 år) innenfor et juridisk område (stat).
 - **hindrer andre** i å produsere, importere og selge oppfinnelsen
 - kan lisenseres/leies ut
- Skal sikre alle tilgang til oppfinnelsen og kunnskapen bak, ved at virkemåten offentliggjøres.
 - Formålet er dermed primært å gi et tidsbegrenset (rettsbeskyttet) monopol til oppfinneren,
 - mot at h@n offentliggjør/publiserer...

Hva kan patenteres?

- En konkret, praktisk løsning på et problem der løsningen
 - har teknisk karakter
 - har teknisk effekt
 - er reproducerbar
- Oppfinnelsen må være **ny**
 - Kan ikke være omtalt i tidligere patenter, tidsskrifter, eller annet noe sted (i verden!), før datoen søknad innleveres.
- Oppfinnelsen må ha **oppfinnelseshøyde**
 - Må skille seg vesentlig fra tidligere kjent teknikk
 - Kan ikke bare være en logisk videreføring av tidligere teknikk...
 - Sett i sammenheng med tidligere publikasjoner kan den ikke være opplagt for en kyndig person

Hvordan få man patent?

- Patentstyret tar i mot søknader (gjennom Altinn)
 - Patentet gjelder kun for Norge dersom det innvilges
 - Samordner også Europeiske søknader til EPC
 - Kostnader: <http://www.patentstyret.no/no/Patent/Hvor-mye-koster-det/>
- Søknader utformes (oftest) av patentbyrå e.l.
 - Koster ~ 20 kkr og oppover

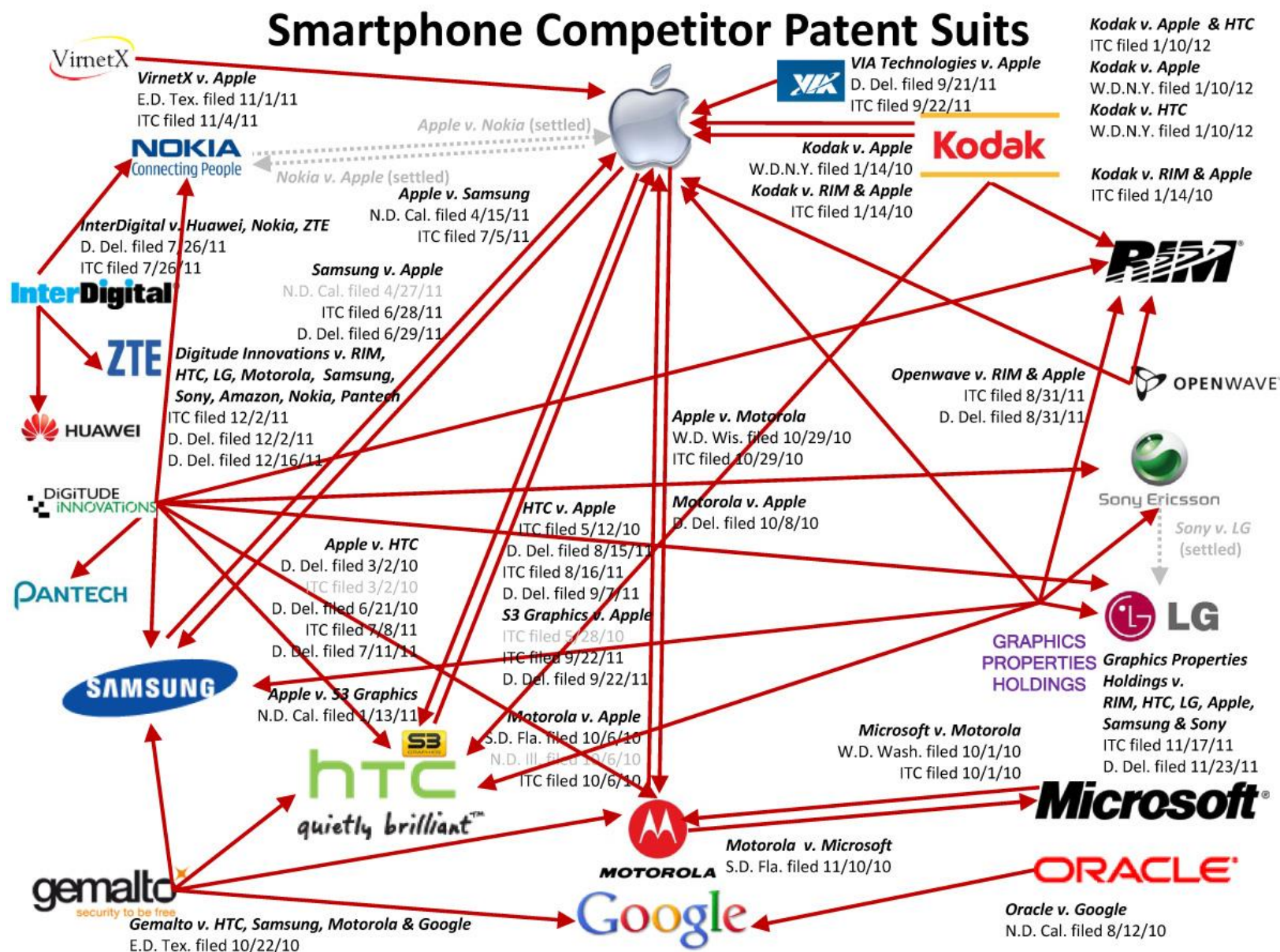
Software-patent?

- Software som **sådan** kan ikke patenteres (EPC Art. 52)
 - Utformingen (kildekoden) er automatisk beskyttet av åndsverksloven (forutsatt verkshøyde)
 - M.a.o. et program er ikke en oppfinnelse
- Tekniske framgangsmåter og apparater, kan derimot patenteres...
 - Man trenger **helt sikkert** hjelp av en patentfullmektig i utformingen av søknaden...
 - Spesielt dersom man ønsker å søke patent i USA...

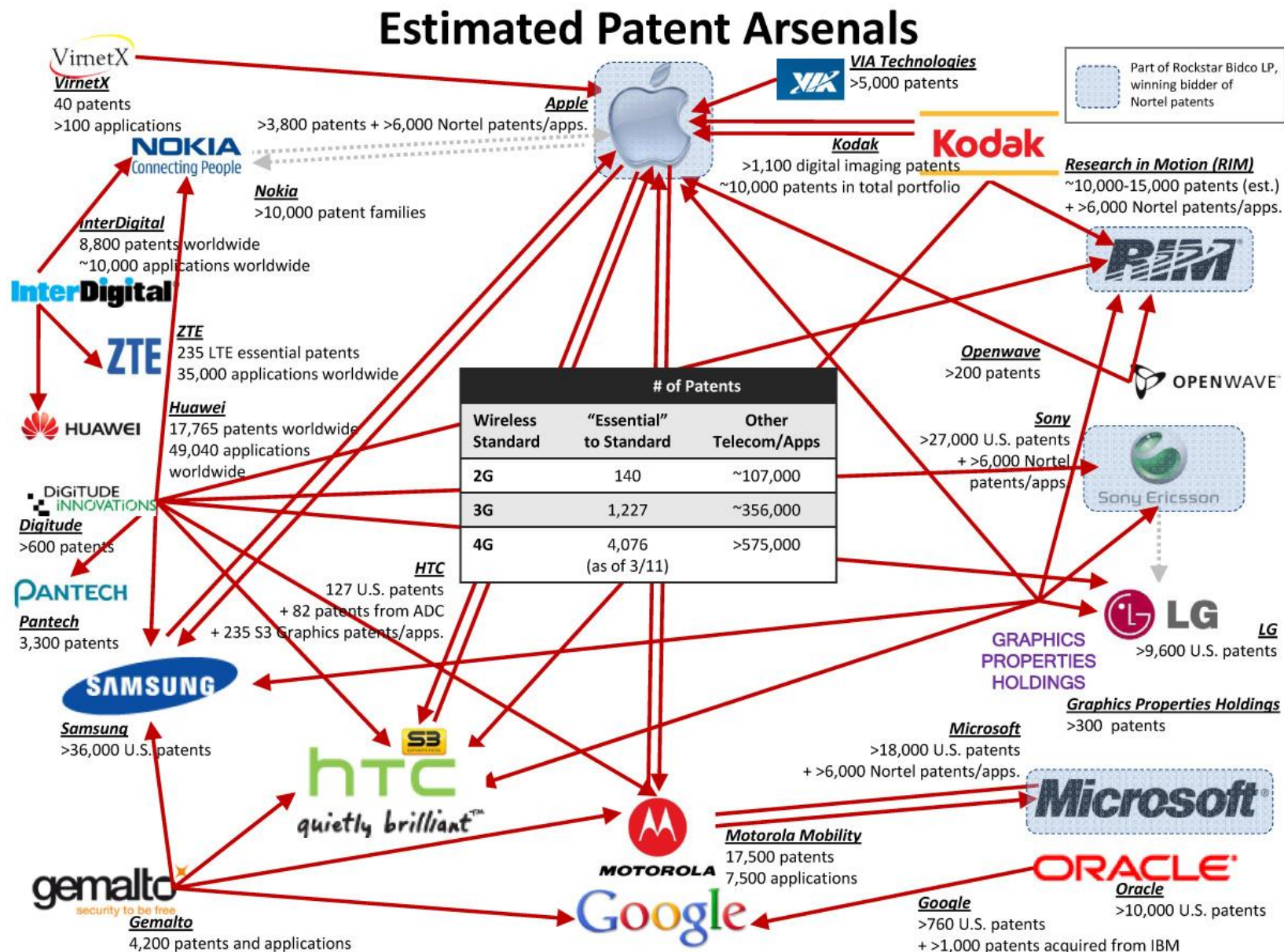
Patent-register

- Patenter skal sørge for offentliggjøring og virke som en «ide-bank»
- USA: [Google Patent Search](#)
- Norge: [Patentstyret](#)
- EU: [European Patent Register](#)
- Dersom du har en ide til noe som effektiviserer, forenkler, ved hjelp av et dataprogram er dette steder å søke.

Patent-»krig» (1)



Patent-»krig» (2)



- Patenter brukes **ikke** bare til å sikre seg egne rettigheter
- Man kan bryte patentrettigheter ubevisst
- Man må også sjekke at man ikke bryter andres patenter!
 - Kan bli dyrt i USA...
 - Der bærer man (nesten) alltid egne rettsomkostninger
 - Dette er i ferd med å endre seg

- Patent i ett land kan være nok til å stoppe et produkt
 - Særlig USA
- Bruker patenter bare for å saksøke
- Motstanderene gir seg fordi det er billigst
- *Alice Corp v. CLS Bank (2014)* avgjorde at “do it on a computer” er ikke nok til å lage en ny oppfinnelse



Open Source Lisensering og CrCo

- Den med opphavsrett til et åndsverk har enerett til kopiering og distribusjon
- Kan lisensiere bort denne («økonomiske») retten
- Copyleft
 - [Gnu General Public License](#) m.fl.
 - Gir deg bare tillatelse til å bruke, endre og distribuere dersom du gjør det med lisensen og gjør endringer mm offentlig tilgjengelige
- F.eks. BSD lisenser stiller ikke like strenge krav til videre-distribusjon som GPL
- **Creative Commons**
 - Standard dokumenter for å gi fra seg ulike «grader» av opphavsrett
 - Jf Youtube



Attribution (by)



Noncommercial (nc)



No Derivative Works
(nd)

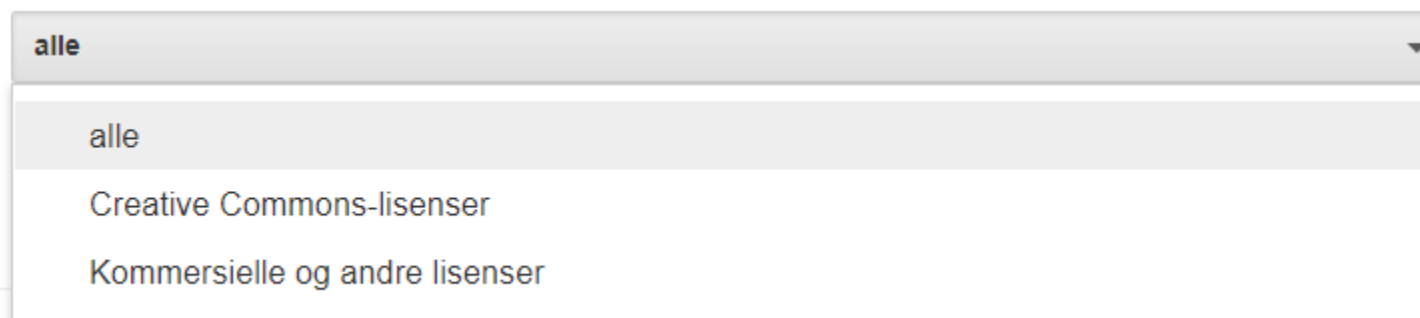


Share-alike (sa)

Finne bilder som er gratis å bruke?

- Man må ikke tro at man kan bruke alle bilder man finner på google, de fleste bilder er beskyttet som åndsverk og kan ikke brukes i kommersiell sammenheng!
- https://www.google.com/advanced_image_search

bruksrettigheter:



Finn bilder du står fritt til å bruke selv.

- OBS; denne var enklere før, da kunne man søke etter «fri bruk, også kommersielt», nå må man sjekke CC lisensen...

DRM

igital ights anagment

DRM (Teknisk kopibeskyttelse)

- DRM (Digital Rights Management) er systemer som begrenser bruken av digitale media
- DRM skal (ofte) beskytte mot lovstridig endring, deling, **kopiering**, utskrift og fremvisning av digitale media
- Noen innehavere/eiere hevder at DRM er nødvendig for å forhindre tapt fortjeneste pga illegal distribusjon av deres åndsverk.

Åndsverk og opphavsrett

- Den som har skapt verket har opphavsrett
 - Kan overdra økonomisk rett ved salg, arv, konkurs...
- Tre krav:
 1. Verk på det litterære, vitenskapelige eller kunstneriske område
 2. Resultat av en individuell, skapende innsats (**Verkshøyde**=originalitet)
 3. Skapt/frembrakt av et menneske (konkret utforming)
- Opphavsretten oppstår samtidig med at verket blir skapt.
 - Verket trenger ikke registreres eller ha copyright-merke for å ha vern.
 - Men: **Dataprogrammer** som er skapt innenfor arbeidsforhold tilhører **arbeidsgiver**(§39 g)

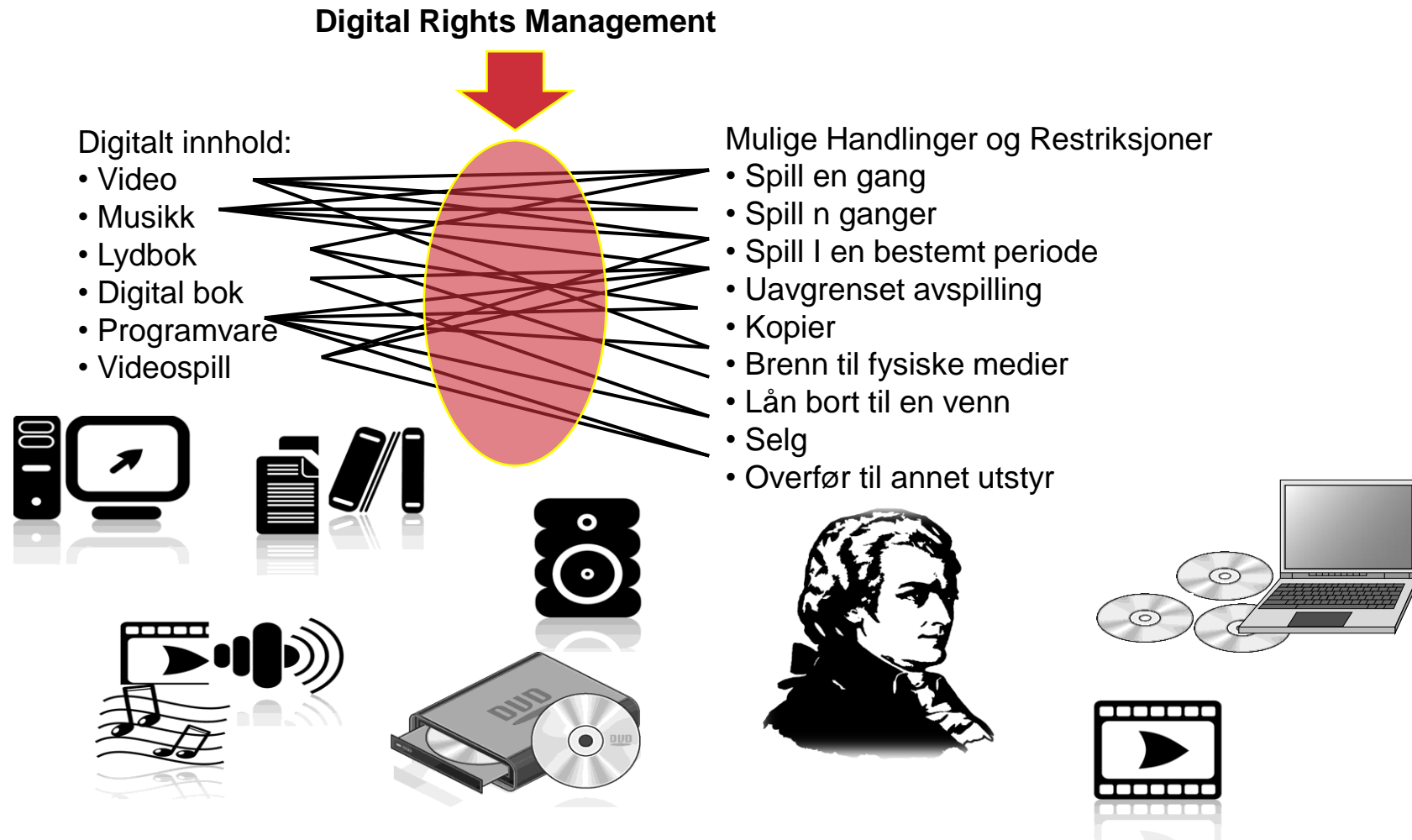
1. Ideelle rettigheter (personlige og evige)

- Rett til å navngitt som opphavsmann
- Respekt-retten: Andre som har fått rett til å bruke verket kan ikke gjøre det på en måte som er krenkende for verk eller opphavsmann.

2. Økonomiske rettigheter (70 år etter død)

- Enerett til å fremstille eksemplarer
 - Alle typer kopiering (analoge og digitale)
- Enerett til å gjøre verket tilgjengelig for allmenheten
 - Opplesning, WWW, ...

- Mange muligheter som må dekkes av DRM



- Fikk i 2005 nye bestemmelser om DRM (EU-tilpassning)

§53a: «Det er forbudt å omgå effektive tekniske beskyttelsessystemer som rettighetshaver eller den han har gitt samtykke benytter for å kontrollere eksemplarfremstilling eller tilgjengeliggjøring for allmennheten av et vernet verk.

Det er videre forbudt å:

- a) selge, leie ut eller på annen måte distribuere,
- b) produsere eller innføre for distribusjon til allmennheten,
- c) reklamere for salg eller utleie av,
- d) besitte for ervervsmessige formål, eller
- e) tilby tjenester i tilknytning til

innretninger, produkter eller komponenter som frembys med det formål å omgå effektive tekniske beskyttelsessystemer, eller som kun har begrenset ervervsmessig nytte for annet enn slikt formål, eller som i hovedsak er utviklet for å muliggjøre eller forenkle slik omgåelse.

« **53b.** Rettighetshaver skal påse at den som har lovlig tilgang til et vernet verk, uten hinder av effektive tekniske beskyttelsessystemer kan gjøre bruk av verket, herunder fremstille nye eksemplarer, i henhold til §§ 13a, 15, 16, 17, 17a, 21, 26-28 og 31.

Dersom rettighetshaver etter begjæring fra berettiget etter bestemmelsene ovenfor ikke gir tilgang som nevnt i første ledd, kan han etter begjæring fra den berettigede pålegges å gi slike opplysninger eller annen bistand som er nødvendig for å muliggjøre bruk av verket i samsvar med formålet...

§ 53c. Omsetning av, eller besittelse i ervervsøyemed av et hvilket som helst middel hvis eneste formål er å gjøre det lettere ulovlig å fjerne eller omgå tekniske innretninger til beskyttelse av et datamaskinprogram, er forbudt.»

Så hva er lov i Norge?

- Det er dermed ulovlig å bryte «effektiv» DRM, men påbudt å ikke gjøre den så effektiv at man ikke kan ta backup / private kopier(?)
- Eller?
 - [Forbruker-rådet spurte ulike eksperter](#)
 - Det var da i all hovedsak uklart hvordan loven skulle tolkes i de fleste interessante tilfeller.
 - Det er det stort sett fremdeles...
- F.eks.: Det kan være ulovlig å lagre innholdet på en web-side uten tillatelse, bortsett fra i skolearbeid (Kopinor) – browser cache... 😊

- ÅVL: «§ 12. Når det ikke skjer i **ervervsøyemed**, kan enkelte **eksemplar** av et **offentliggjort** verk fremstilles til **privat bruk**. Slike eksemplar må ikke utnyttes i annet øyemed. Opphavsmennene gis en **rimelig kompensasjon** gjennom årlige bevilgninger over **statsbudsjettet**.»
- Kompensasjonen gjøres (hovedsaklig) gjennom organisasjoner som forvalter lisenser
 - Kopinor, Tono, osv.
 - Se også <http://www.clara.no>

DVD-Jon-saken

- Jon L. Johansen (1983-)
- Utviklet sammen med andre DeCSS systemet for dekryptering av DVDer
- DVD Copy Control Association og Motion Picture Association anmeldte ham til Økokrim som reiste sak i 2002. (Straffelovens § 145)
- Først frikjent i Oslo byrett, så (etter anke) i Borgarting Lagmannsrett (2003)
- Ville sannsynligvis blitt dømt i dag (Åndsverksloven oppdatert 2005).
- Se <http://www.doubletwist.com/>



Kopibeskyttelse: Metoder

- **Dongle**

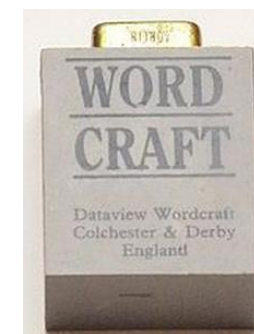
- HW-utstyr som må plugges inn og inneholder nøkkel/kryptoprosessor (jf TPM) som kreves for å kjøre programvaren



- **Produkt-nøkkel**

- Legges inn under installasjon
- Testes online for duplikat
- Lisensen knyttes til maskinen v.h.j.a. OS- eller HW-signatur

WEBEVAL-901C-4D17-CD86-B812-2B6A



- **Telefon-aktivering**

- Må ringe opp og snakke med noen («avskrekking»)



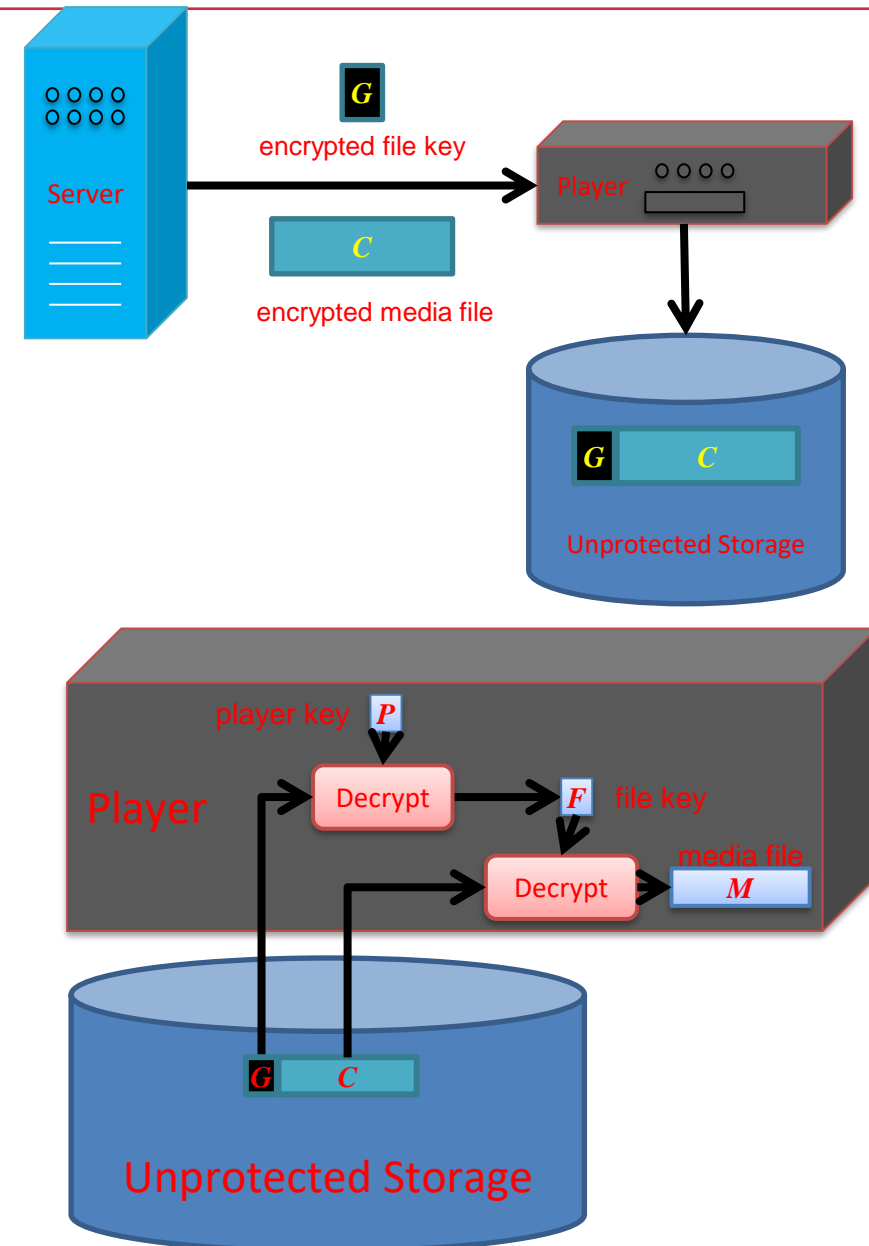
Analogt hull

- De fleste former for kopibeskyttelse har «analoge hull»: sårbarhet for innspilling under avspilling.



DRM media fil distro

1. Media server sender filen kryptert med filnøkkel, og filnøkkel kryptert med avspiller-nøkkel
2. Avspilleren dekrypterer først filnøkkelen med spillernøkkelen, så mediafilen med filnøkkelen



- CD/DVDer er vanligvis kopi-beskyttet
- Det er (sannsynligvis) lov å lage en backup
- De fleste beskyttelsesmekanismene er basert på kryptering
 - Og har blitt knekt
- Firmaene har (kanskje) i realiteten gitt opp å stoppe andre en «vanlige» brukere fra å kopiere
 - Hvordan så stoppe «proffer» fra å dele med alle via (f.eks.) Torrents?

- USA: Media-industrien ønsker å ansvarliggjøre ISPer og utvide mulighetene til å stenge ned og sensurere de som forbryter seg mot opphavsretten
 - F.eks. fjerne DNS, filtrere Google osv.
 - Ikke avgjort i Kongress eller Senat pr d.d.
- ACTA (Anti-Counterfeiting Trade Agreement)
 - Internasjonal avtale for å stoppe falske merkevarer, medisiner og opphavsrettbrudd
 - Undertegnet av de fleste større industriland
 - Kun ratifisert i Japan foreløpig
 - EU parlamentet stemte den ned i Juli 2012
 - Resultat av hemmelige forhandlinger og uklart hva den i praksis vil bety

Tillegg til åndsverksloven 2013

- I 2009 tapte TONO og flere andre en sak mot Telenor der de krevde stengning av tilgang til The Pirate Bay
 - Lagmannsretten begrunnet tapet med at norsk lov ikke åpnet for å pålegge Telenor noe slikt.
- 2. September 2015 ble resultatet motsatt.
- Nylig (2013) ble åndsverksloven endret slik at:
 - a) IP-adresser brukt til rettighetskrenkelser kan registreres uten søknad til Datatilsynet.
 - b) Rettighetshaver kan gå til retten for få utlevert personopplysninger fra ISP basert på IP-adresse
 - c) Domstol kan pålegge ISP'er å hindre/vanskeliggjøre tilgang til nettsteder som krenker opphavsrett.

Ytringsfrihet?

- Et gjentakende spørsmålet i mange sammenhenger her er dermed forholdet mellom **IP** (Intellectual **P**roperty rights) og ytringsfrihet
 - Hvor **går** grensen?
 - Hvor **bør** den gå?
- Ikke bare et **juridisk**, men også et ideologisk og **etisk** spørsmål.
 - Jf «The great firewall of China».



Epost og spam



- Sendes med (E)SMTP
 - Se TK1100
 - Ingen (innebygde) garantier for konfidensialitet, eller autensitet
 - Kan utvides med SSL/TLS (konfidensialitet)
 - Beskytter mot avlytting «på linja»
 - SMTP-server fremdeles sårbar
- Autentisering av meldingen
 - Kan autentisere bruker, eller organisasjon
 - Organisasjon enklere, og i stigende bruk
 - «Web of trust»: PGP
 - Hierarkisk a la TLS: S/MIME, DKIM



Por que ela não ela não come ovo,
bacon, SPAM e linguiça?

«Web of trust»

- Basert på (personlig) etablert tillit til nøkler

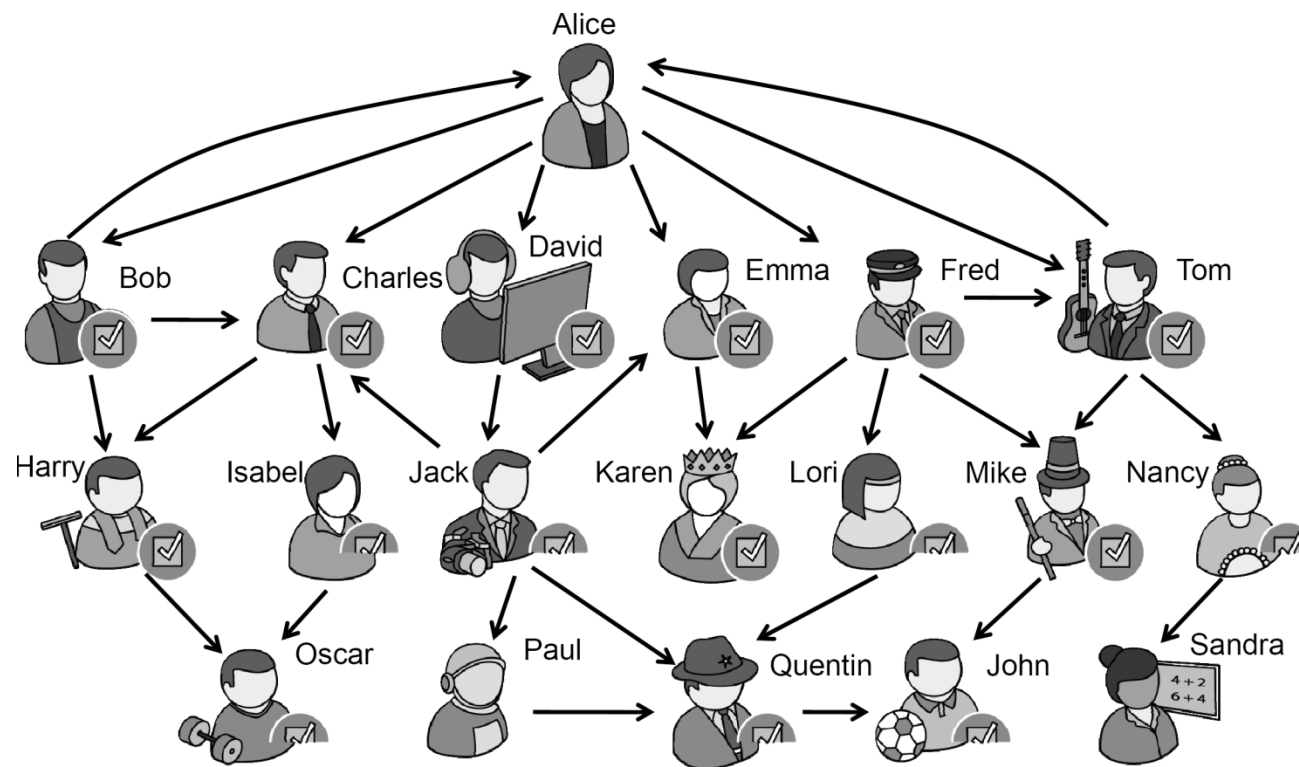
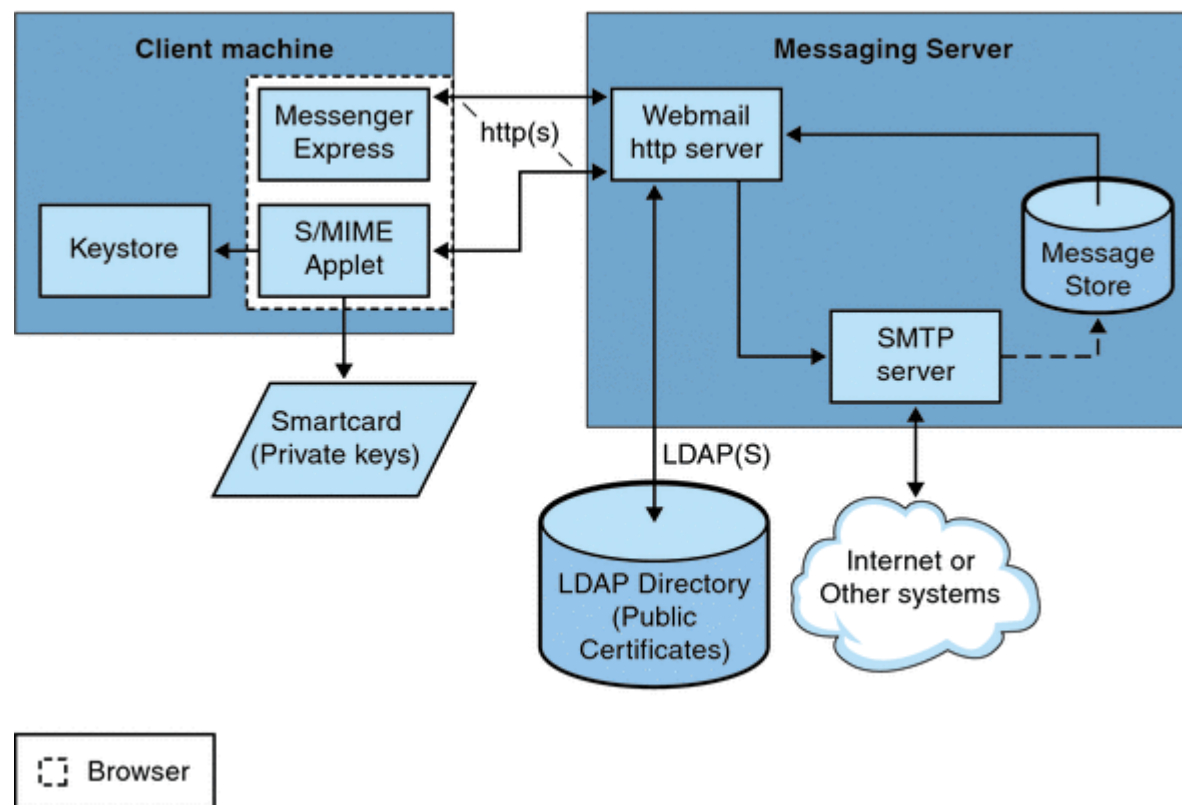


Figure 10.5: A web of trust in PGP. A directed edge from A to B indicates that A signs B 's key. A full check mark indicates a key Alice fully trusts and a half check mark indicates a key that Alice partially trusts. People without a check mark or with half check mark have no keys that Alice trusts.

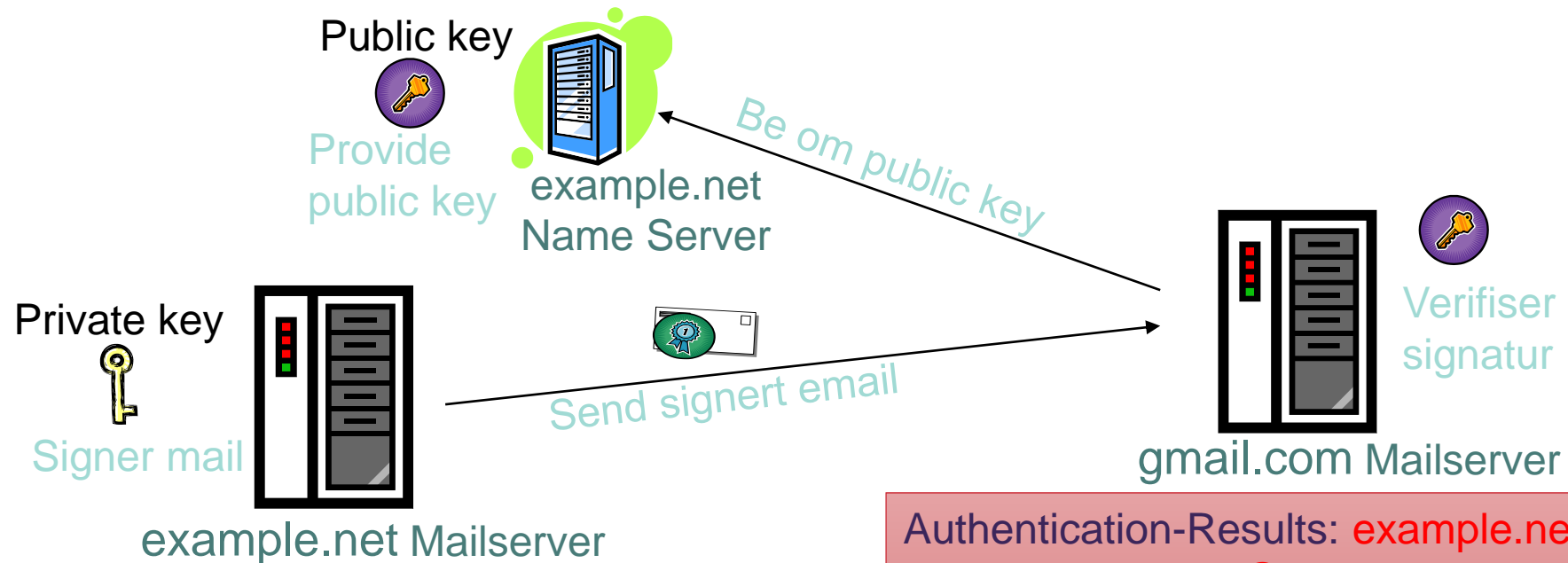
- «Personlig»
- Kan brukes både til kryptering og signering
- Basert på hierarkisk sertifikat-tjeneste



- DomainKeys Identified Mail (DKIM)
- Vanligvis serveren som signere og verifiserer
- Basert på DNS (TXT RR)
- Signerer også header-feltene (FROM: osv)
- F.eks. Gmail godtar ikke epost fra paypal.com og eBay uten gyldig DKIM signatur

DKIM-Signature: v=1; **Algoritme** a=rsa-sha256; **Domene og nøkkel-id** c=relaxed/relaxed; d=brown.edu; s=cs;
h=domainkey-signature:mime-version:received:in-reply-to:references
:date:message-id:subject:from:to:cc:content-type; **Signerte headere**
bh=L+J52L7uTfKTeI/+2ywqQMH1eiGvl6tsXjDNAySew+8=; **Hash av meldingskropp**
b=vE2bvcj8GVHGHeECJA4WJ/t1BRbLBvITQywbZI/HgFSMRfoIVUvH9lyVeMitOaNMeQ
C29TNP5fJPphaFhHb9tf8EkJBlojRryWRAI5/r5RgT6z5DLWs8fgHe0wUbWEwBQ+sSTs
A+vbfuLObS1Gwdxtu81HNOfiSLY0u2CM6R31s= **Signatur**

- Skal sende DKIM-sikret epost fra bol@example.net til bengt@gmail.com



DomainKey-Signature: a=rsa-sha1;
s=mail; d=example.net; c=simple;
q=dns; b=Fg...5J

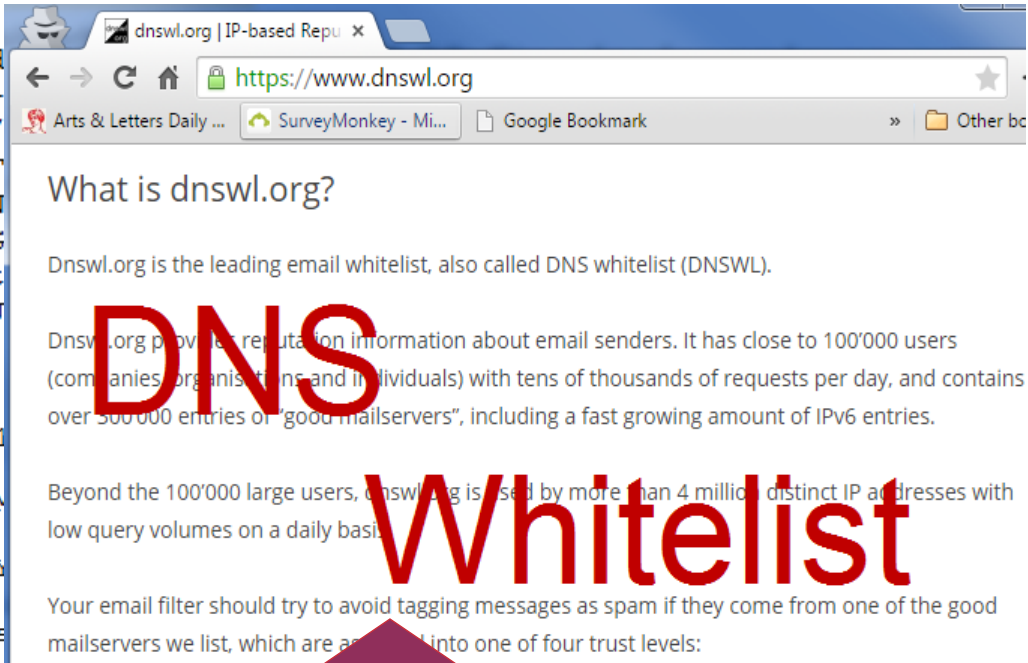
Authentication-Results: example.net
from=bol@example.net;
domainkeys=pass;

Gmail («Show Original)

X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=google.com; s=20120113;
h=mime-version:date:message-id
:content-transfer-encoding:x-
bh=kCgE3A+bu5ezIZYoduP/QqklyY/
b=CMjgJ8gKcKBpH9dYfAx+XsJmcLlF
QwRh16IbOMpRjWZfzwp30tIZWhC5N
KnarGrbmHtqH7PIoiV6vtQuh2H+cG
jc/6xWlvRBVRoOEIKfOt76tulguBt
dBMrXJYba7IN9yRnHWmlZVl/i0XFJ
OaJQ==

MIME-Version: 1.0
Received: by 10.50.192.137 with SMTP id hg9mr1
15 May 2012 01:58:28 -0700 (PDT)
Received: by 10.43.43.136 with HTTP; Tue, 15 M
Date: Tue, 15 May 2012 10:58:28 +0200
Message-ID: <CANXofSE2eU1jsjK=4Lu7fhD+jSNWYtnY
Subject: TEst
From: =?UTF-8?Q?Bj=C3=B8rn_Olav_Listog?= <blis
To: bjorn@listog.no
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
X-Gm-Message-State: AL0CoQmG9TsZtGUnrOo0O99P6txJo/pp1g8Jzn2rJ85_HbKCqsRlVZ1Dgo8vfEG/Jzyl6y
X-Spam-Status: No, hits=-0.2 required=5.0
X-Spam-Report: -0.2 hits, 5.0 required;
* -0.7 RCVD_IN_DNSWL_LOW RBL: Sender listed at http://www.dnswl.org/, low
* trust
* [209.85.213.175 listed in list.dnswl.org]
* 0.5 NULL_IN_BODY FULL: Message has NUL (ASCII 0) byte in message
X-Virus-Scanned: by moam (http://www.moam.net/)
X-Moam-Version: 0.95

Dette er en test



What is dnswl.org?


Dnswl.org is the leading email whitelist, also called DNS whitelist (DNSWL).

Dnswl.org provides reputation information about email senders. It has close to 100'000 users (companies, organisations and individuals) with tens of thousands of requests per day, and contains over 500'000 entries of "good mailservers", including a fast growing amount of IPv6 entries.

Beyond the 100'000 large users, dnswl.org is used by more than 4 million distinct IP addresses with low query volumes on a daily basis.

Your email filter should try to avoid tagging messages as spam if they come from one of the good mailservers we list, which are assigned into one of four trust levels:

DNS Whitelist



?

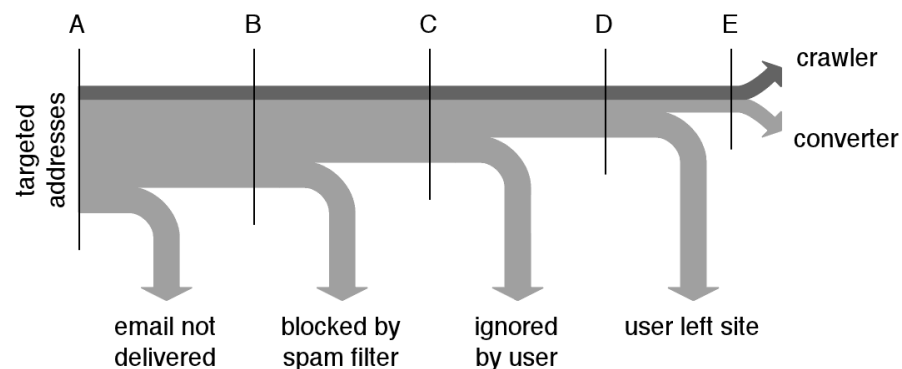
Epost spam?

- Epost o.l. som
 - Massekorrespond
 - Uønsket/uoppfordret
- Er det lov?
 - Markedsføringsloven §2b: «*Det er forbudt i næringsvirksomhet uten mottakerens forutgående samtykke å rette markedsføringshenvendelser til fysiske personer ved hjelp av elektroniske kommunikasjonsmetoder som tillater individuell kommunikasjon, som for eksempel **elektronisk post**, telefaks eller automatisert oppringningssystem (talemaskin).*»
 - EUs kommunikasjonsdirektiv (implementert i Norge 2005) tillater dog at næringsdrivende som har etablert et kundeforhold kan sende ut markedsføring for tilsvarende produkter med e-post/SMS/MMS uten uttrykkelig samtykke.
 - Jf Ehandel-loven
- USA: CAN-SPAM (2003)
 - Forbyr falsk og forvirrende info i header-feltene
 - Forbyr misvisende Subject:-felt
 - Påbyr mulighet for avmelding
 - Porno skal merkes som det i Subject:
- Se også [Forbrukerombudets Guide](#)

- Høsting av adresser
 - Automatisk («spidering»)
 - Legg alltid ut epostadresse i format som er vanskelig å identifisere:
 - bengt (at) h-ck (dot) me
 - Eller som et bilde
 - Sjekk alltid «privacy policy» før du registrerer deg på nettsteder
- Epost-lister selges
 - Mer verdifulle dersom segmentert i kundegrupper...

Spam er det lønnsomt?

- ~ gratis å sende store volum
- Kanich & al. infiltrerte og undersøkte spam sendt ut av Storm botnettet
 - 347.590.389 eposter sendt over 1 måned
 - = 28 betalende «kunder» = \$ 3000
 - I.e. konverteringsrate = 0,0001%



STAGE	PHARMACY	
A – Spam Targets	347,590,389	100%
B – MTA Delivery (est.)	82,700,000	23.8%
C – Inbox Delivery	—	—
D – User Site Visits	10,522	0.00303%
E – User Conversions	28	0.0000081%

Captcha

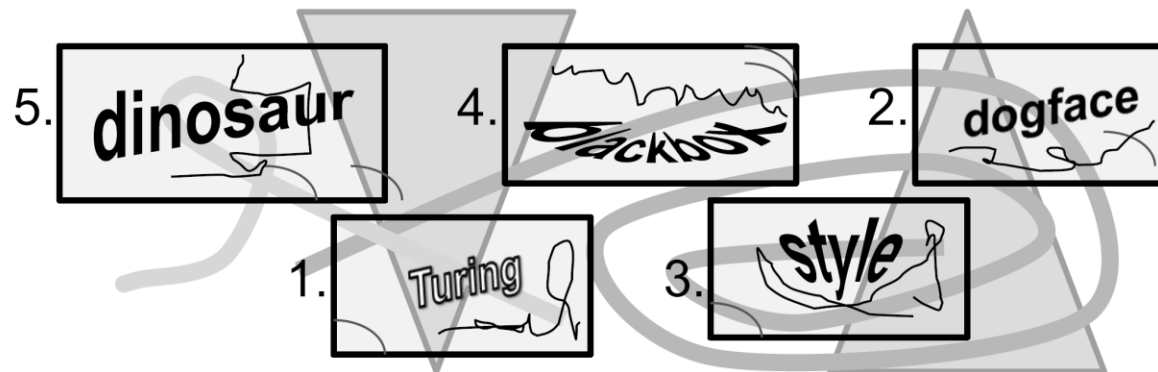
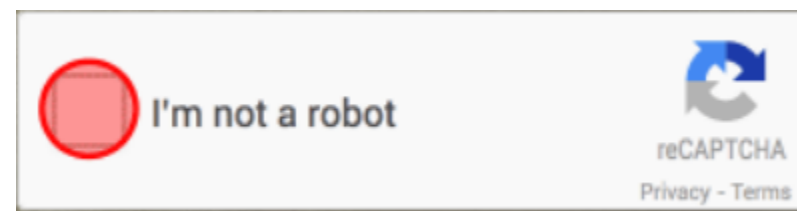


Figure 10.8: A CAPTCHA. Asking a user to type the words they see inside the rectangles, in the specified order, is something that is relatively easy for a human to do compared to a computer.

- For å vanskeliggjøre automatisk opprettelse av webmail-kontoer o.l.
 - Ikke vanskelig å komme forbi, men øker kostandene for spammer'ne
- Google's nyeste reCAPTCHA sjekker også adferd på brukeren...

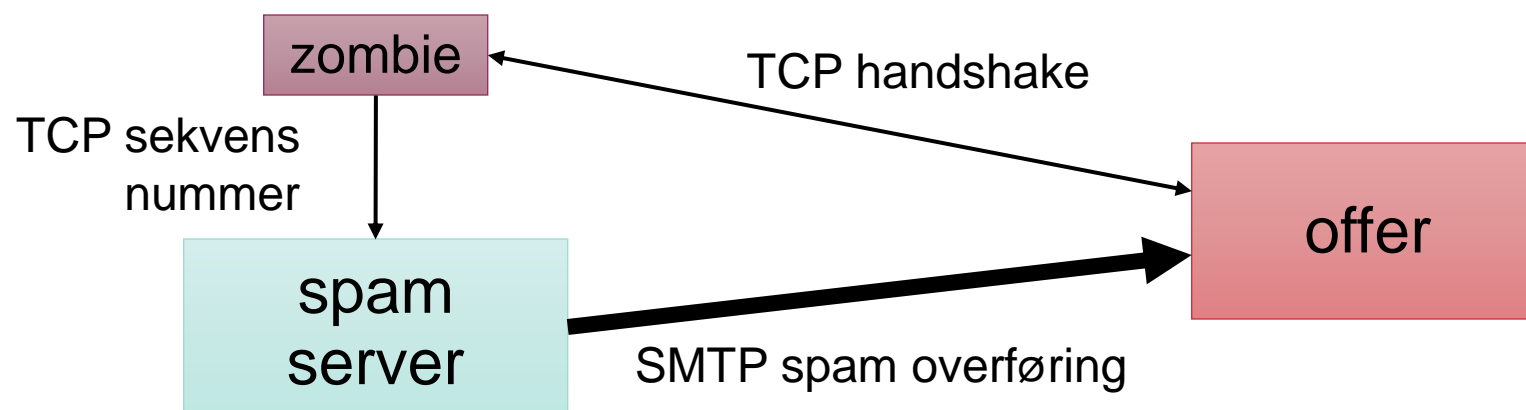


Svarte- og Hvite-listing

- F.eks. Spamhouse Black List (SBL)
 - Database med IP-adresser til spam-kilder
 - Fjerner ca 10% av spam'en før den blir overført
 - Rutiner for å melding, oppføring og fjerning
 - Problem med «falske positive», se IDS i F06
- F.eks. DNS Whitelist
 - Liste over ca 150000 «gode epost-servere»
 - Benyttes f.eks. av Gmail sammen med Bayesiansk filtre (hvilke ord tyder på spam med hvilken sannsynlighet mm)

Hvordan unngå lister

- Spoofing
 - La en liten zombie initiere TCP-forbindelsen
 - Ikke på IP-svarteliste, eller innenfor pålitelig domene
 - Overfør TCP-sekvensnummer til server
 - Send spam med spoofet IP-adresse og TCP-nummer



Grålisting («greylisting»)

- Spam servere sender typisk ikke meldinger om igjen ved feil og forespørsel om å vente
- SMTP kan konfigureres til å avvise epost fra ukjente avsendere på første forsøk («temporary rejection»)
 - Vanlige SMTP-tjenere vil da forsøke på nytt etter en periode
 - Spammere vil vanligvis ikke bruke ressurser på å sende om igjen
 - Medfører dog forsinkelser for brukerne...

- Svarteliste på enkeltord («signatur»)
 - Medfører for mange falske positive
 - Lett å omgå ved feilstaving, bruk av bilder o.l.
- Bayesiansk filtrering («heuristikk»)
 - Lærer opp filteret til å skille mellom ekte og spam.
 - Tilegner sannsynlighet for spam til ord
 - Beregner sannsynlighet for spam basert på kombinasjon av verdier
 - Admin setter grenseverdien for utfiltrering

INTERNET OF THINGS

Internet of Things

- I fremtiden (dvs i dag) er det forventet at alle ting skal være koblet til Internett
- Det vil si at alle ting har en IPv6 adresse, og kan både sende til og motta fra Internett
- Stekeovner, kjøleskap, kaffetraktere, baby monitorer, dørlåser, for å ikke glemme BILER, og – tja – lyspærer...

Erfaringsoppbygging SW

- Software bransjen har siden 80-tallet utviklet programvare, og blitt angrepet av hackere og malware
- Mye kollektiv erfaring er opparbeidet innen sikkerhet, «do's and dont's» i bransjen
- Dette er en lang prosess, og «smitter av» fra seniorer til juniorer
- Kryptering, least privileges, buffer overflow beskyttelse, osv er viktige erfaringer

vs hvitevare bransjen

- Hvitevare bransjen, og andre rene tekniske vareprodusenter, har alltid laget kretskort for å styre tekniske varer
- Kretskort utviklere har et helt annet erfaringsgrunnlag – ikke noe behov for sikkerhet, men fokus på ytelse på kretskort
- Plutselig ble datamaskiner små nok til å integreres i andre produkter enn datamaskiner – EN chip med CPU, minne, disk, nettverk, og et OPERATIVSYSTEM

vs hvitevare bransjen #2

- Kretskort utviklere blir nå satt til å utvikle software som skal kjøre på en embedded Linux device – som skal være på Internett
- Utviklere som lager software til IoT på kjøleskapet og lyspærene har ikke erfaringen fra sikkerhet som du forventer av alt annet som er på Internett...
- Dette baner vei for alle de «gamle» sårbarhetene på nytt – på nye enheter

DDoS fra Internet of Things

- 20. september 2016 ble det til da kraftigste DDoS angrepet gjennomført
- Angrepet er anslått til å ha vært 990 Gbps
- Bak angrepet stod 150.000 CCTV kameraer, som var koblet til internett og var blitt hacket
- Etter å ha avslørt mennene bak ble «som takk» Brian Krebs' nettsted angrepet med 620 Gbps med søpletrafikk

Philips lyspærer

- 3 israelske researchere offentliggjorde i November 2016 en rapport 'IoT Goes Nuclear: Creating a ZigBee Chain Reaction' hvor de angriper Philips Hue
- De har laget en proof-of-concept orm som kan spre seg fra lyspære til lyspære og kontrollere lyset, i teorien kan de ta ned lyset i en hel by
- Philips hadde brukt samme AES-CCM nøkkel i alle lyspærene de produserte...

Tesla elektriske biler

- At Tesla har avanserte biler vet alle
- Keen Security Lab demonstrerte i September 2016 at de kunne ta kontroll over CAN Bussen i Tesla, og aktivere bremsene på bilen fra avstand
- De hadde også full kontroll på dørene, bagasjelokk, flytte på setene, aktivere blinklys og vindusviskere – og folde inn sidespeil, som ikke er mulig når bilen kjører
- CIA sitt Vault-7 har også jobbet med remote kontroll av biler, for å utføre attentat!!!

Creepy eye on the wall

- I November 2016 ble de slått opp en sak fra USA hvor en mor kom inn i rommet til barnet, og hørte en stemme i baby monitoren si «Wake up little boy, daddy's looking for you»...
- Barnet hadde klaget over at han var redd på natten fordi «telefonen pratet til ham»
- Noen hadde hacket baby monitoren og fulgt med på – og pratet med barnet over lengre tid, hva har han sagt og hva var planen?!
- <http://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/>
- <https://www.buzzfeed.com/craigsilverman/creeps-hack-baby-monitors-and-say-terrifying-thing>

Kaffemaskiner – med mer enn kaffe

- Land har alltid spionert på hverandre
- Avlyttingsutstyr har vært forsøkt plantet hos «fienden» siden de ble oppfunnet, også gjemt i gaver – ref «The Thing» fra August 1945 til US Embassy i Moskva
- Men når vi er så paranoide i dag, så sjekkes alt grundig, spesielt gaver – men hva med ting ansatte kjøper privat og tar med seg?
- I Russland fant man avlyttingsutstyr i kaffemaskiner og strykejern som var kjøpt i butikk – kineserne hadde tilsynelatende avlyttet ALLE modellene som ble produsert i Kina for det russiske markedet!

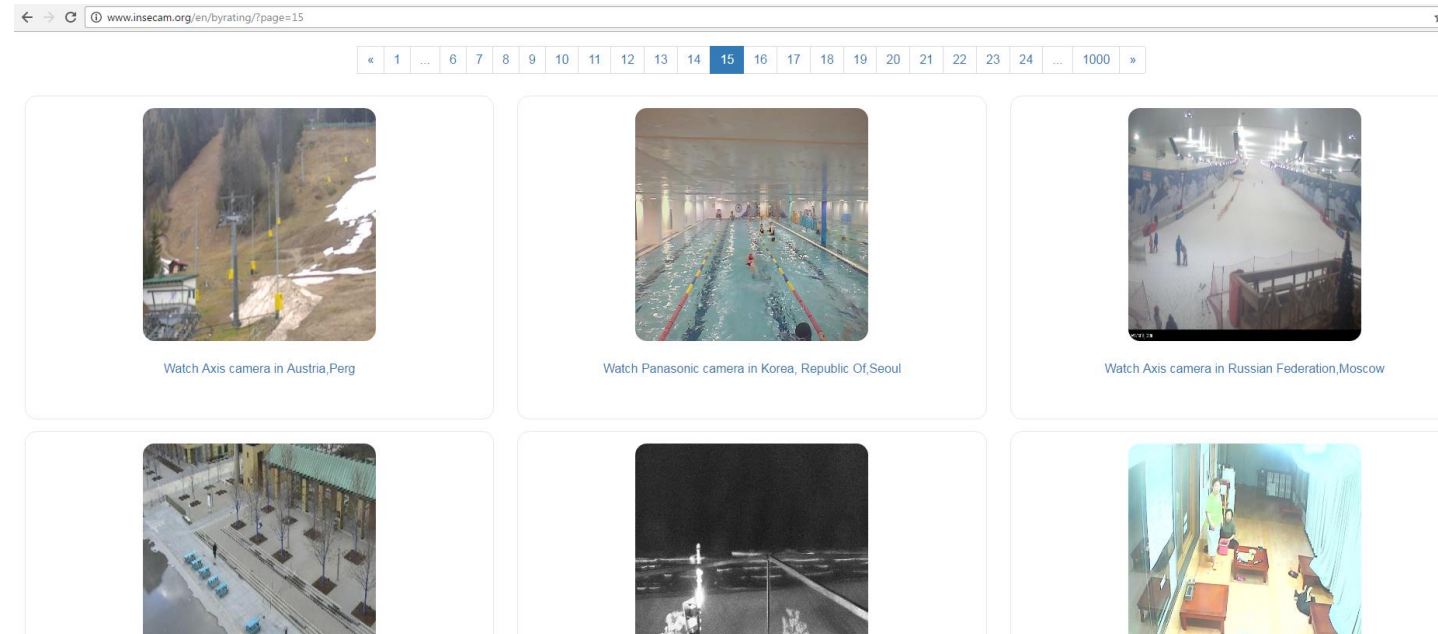
Rossiya 24 avslører

- Har du sjekket DITT Made-In-China strykejern for avlyttingsutstyr?



Kameraer «på internett»

- Et utall kameraer kan kjøpes til privat overvåkning, de fleste med en app eller annen software for å styre og overvåke
- Hvor mange bytter standard passordet?
- Enkelt bruk og «med internett tilkobling» trenger ikke være positivt!



Dagens øvingstime?

- Oppgavesett ligger i Canvas
- Skrive en 1 sides drøfting om fordeler og ulemper med patent og kopibeskyttet software. Hvem tjener på det og hvem taper? Kan en aktør både tjene og tape på streng håndheving av kopibeskyttelse?
- Begynne å forbrede til eksamen, gå gjennom tidligere forelesninger
- Tidligere eksamener er lagt ut i Canvas

- Defensive Programming
 - Typiske programmeringsfeil
 - Viktighet av input validering
 - Typiske server konfigurasjonsfeil
- Eksempler på sårbarheter
 - Hentet fra ekte penetrasjonstester
- Uken etter har vi repetisjonsforelesning