Det finnes ingen gjemmesteder på elektroniske veier

Professor Gunnar Hartvigsen

Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet
Universitetet i Tromsø

Utgangspunktet

- De fleste er ikke klar over graden av overvåkning de utsettes for på Internett samt hvor vanskelig det er å skjule sine spor
- Det er lett å føle seg overvåket på Oslo S – mer enn 200 overvåkningskameraer følger dine bevegelser
- Det er vanskeligere å forstå graden av ”overvåkning” på
  - Internett (e-post, news, chat, irc, etc.)
  - en vanlig bytur – gjennom mobiltelefonen, bompengebrikken, e-busskort, elektroniske spor fra betalingsterminaler (bankkort, bensinkort, etc) og fordelskort (Domino, Trumf, Forbrukersamvirke)

Påstand

- Både Orwell og Huxley fikk rett
  - Orwell: vi er utsatt for en massiv overvåkning
  - Huxley: vi forherliger overvåkningen (teknologien)
- To hovedtyper overvåkning:
  - Samtykket – bevisst eller ubevisst
    - Eks. Kortselskapenes informasjon om handlemønster,
  - Ulovlig
    - Eks. Krysskobling av databaser, sporing av signaler, virusprogrammer

Teknologiske muligheter

- Kommunikasjonsutstyr (telefon, mobiltelefon, datakommunikasjon, GPS, etc.)
- Elektroniske transaksjoner (bankkort, fordelskort, adgangskort, etc.)
- Overvåkningsutstyr (mikrofon, kamera, video)

Echelon

- NSA's ECHELON system er designet for å fange opp ordinær e-post, fax, telex og telefonkommunikasjon i verdens telekommunikasjonsnett.
- ECHELON er primært designet for ikke-militære mål: regjeringer, organisasjoner, selskaper og enkeltpersoner i de fleste land.
- ECHELON angår ethvert individs kommunikasjon over landegrensene (og noen ganger innelands) verden over.

Echelon

- ECHELON er ikke designet for å lytte på en spesielt persons e-post eller fax. Systemet gjennomgår store mengder kommunikasjon og forsøker å skille interessante meldinger fra uinteressante
- ECHELON har etablert en kjede med hemmelige lyttestasjoner som overvåker alle internasjonale telekommunikasjonsnett. Noen overvåker telekommunikasjonssatelitter, andre landbaserte kommunikasjonsnett og andre radiokommunikasjon. ECHELON knytter all informasjonen sammen og sørger for at USA og dets allierte kan lytte på det meste av klodens kommunikasjon.

Echelon

- ECHELONs datamaskiner (Dictionaries) søker gjennom millioner av meldinger og finner de som inneholder spesielle søkeord (navn, lokaliteter, tema, etc). Flere medlemsland overvåker også telefontrafikk (tale) (gj. stemmegjenkjenning).
- Datamaskinene har søkeordlister for alle medlems-organisasjoner (NSA, GCHQ, DSD, CSE, XXX)
- Datamaskinene er knyttet sammen via krypterte linjer som er koblet opp mot de fem hovedkontorene i Washington, Ottawa, Cheltenham, Canberra og Wellington.

Kan vi ikke bare kryptere?

- Tung kryptering (128++ bit) kunne vært løsningen. Men dersom ikke denne er tett knyttet til operativsystemet, dvs. at OS'et tar seg av all kryptering/dekryptering, så vil kryptering for de fleste være for arbeidskrevende.
- Hvorfor ikke stole på leverandørene? Fordi: Det av ulike kan være lagt inn bakdører eller forenklinger
  - Microsoft blir beskyldt for å ha lagt inn en egen krypteringsnøkkel til NSA
  - GSM benytter ikke 56 bits krypteringen – de 10 siste er 0'ere

Har NSA en bakdør til Windows?

- Aug 99: I en oppgradering av Windows NT (SP5) glemte programmererne å fjerne navnet på en variabel. Dens navn, _NSAKEY, og det faktum at innholdet er en kryptonøkkel, har satt fart i spekulasjoner om at Microsoft har lagt inn en bakdør for USAs spionorganisasjon, NSA.
- Andrew Fernandes, Cryptonym Corp., hevder å ha avslørt en bakdør inn til Windows, hvor NSA kan være den tredjepart som sitter på nøkkelen.

Har NSA en bakdør til Windows?

- Det har lenge vært spekulert i at Microsoft har latt NSA få legge inn det de behøvde for å overvåke og spionere kloden rundt, men det har aldri vært mulig å bevise det.
- Spekulasjonene har blant annet fått næring av det faktum at det i alle Windows-versjoner ligger minst to kryptonøkler, mens det strengt tatt bare skulle være bruk for én -- for Microsoft og Windows selv.
- Spekulasjonene har gått på hvem som sitter på den andre nøkkelen, og den heteste kandidaten har vært NSA.
- Det viktigste funnet er navnet på variabelen - *_NSAKEY*.

Ikke første bakdør i et OS

- Dersom det stemmer at det eksisterer en bakdør i Windows (95, 98, NT, 2000) så vil det ikke være første gang det installeres en bakdør til et operativsystem.
- Det var i mange år en lite kjent bakdør til operativsystemet Unix. Bakdøren ble lagt inn i rutinen **debug** av vedlikeholdshensyn. Årsaken var at utviklerne var lei av brukere som glemte passordet. Derfor la de inn en mulighet for å logge seg inn som root ved hjelp av en bestemt konto som ikke krevde passord.
- Rutinen var bare kjent i de innerste guru-kretser i Unix-miljøet. Den er senere blitt utnyttet av hacker, m.fl.

Betalingskort forteller det meste

Til de som ønsker å lytte?

Nasjbet

- Da Australia (80-tallet) forsøke å innføre et generelt adgangs- og betalingskort som naturligvis også ville etterlate seg elektroniske spor overalt, ble det, nærmest et folkeopprør.
- Norge (noe senere): Nasjbet – ingen reagerte. (Prosjektet ble stoppet, men da av finansielle grunner. Offer for jappetidens fall?)

Ditt hemmelige bankkort

- Når du trekker bankkortet gjennom betalingsterminalen og slår din pin-kode på buteikkens terminal, da har du i realiteten gitt butikken all den info som er nødvendig for å reproduser kortet.
- Ifi et prosjekt hvor pin-koden trykkes på eget kort og ikke overlates til butikkens terminaler.

Falsk minibank

- Falsk minibank i Buckland Hills Mall in Manchester, Connecticut, 1993.
- PIN & kontonummer ble lagret
- Gjerningsmennene ble tatt etter analyse av overvåkningsfiler fra minibanker
- Gevinsten var på mer enn $100.000

Bankene gjør feil

- For noen år siden ble kontoen til et ektepar tappet for £40 mens de var på feriereise. Banken hevdet at uttaket var gjort av parets datter, som hadde hatt tilgang til kortet mens foreldrene var bortreist.
- Banken nektet selvsagt for at dette kunne være deres feil. Det var umulig! I rettssaken som fulgte ble datteren anbefalt av sin advokat å tilstå uttaket.
- Noen måneder senere ble det imidlertid oppdaget at en av bankens funksjonærer hadde gjort en feil.
- Det tragiske i saken var at da hadde datteren var forsvunnet.

Mobiltelefonen avslører deg

”Don t leave home with it!”

Spritsmuglere

- Våren 1998: politiet knep noen spritsmuglere fordi de hadde mobiltelefonen på slik at man kunne finne ut hvilke basestasjoner telefonen hadde vært i kontakt med (litt forenklet).
- GSM systemet vet din posisjon med 200 meters nøyaktighet. (GPS 10 meter)

Geiranger

- I etterforskningen i drapet på en ung kvinne i Geiranger fikk politiet rettens kjennelse på å få utlevert navnet til eierne av alle mobiltelefoner som hadde vært i Geiranger den dagen kvinnen ble myrdet.

Sørlandsmordet

- 1998: En drapsmann ble tatt på Sørlandet fordi han ringte med avdødes mobiltelefon (men med sitt eget abonnement).
- Det at telefonene nå også sender serienummeret kan være svært nyttig for politiet.
- NetComs ringkontant-ordning hvor man ikke registrer brukeren blir vel på denne måten noe mindre problematisk.

Orderud saken

- 1999: Pensjonistekteparet Orderud og deres datter blir skutt ned og drept i parets hjem. Sønnen, Per Kristian Orderud, er blant de mistenke.
- I etterforskningen blir bl.a. utskrifter fra mobiltelefonsamtaler og logger fra Telenor gransket. To av de siktede – Lars Grønnerud og Kristin Kirkemo har iht mobiltelefon-registrene (nær et) alibi for mordnatten.
- Forklaringene til de siktede prøves mot mobiltelefon-registrene for å få bekreftet/avkreftet forklaringene til de siktede.

Orderud saken

- Dagbladet 18. august 1999:
- Utskriftene viser at Kirkemo ringte ut eller mottok samtaler bortimot 15 ganger mellom midnatt og 06 drapsnatta.
- Men det finnes et tidsrom på en time og 50 minutter da telefonen ikke var i bruk. Teoretisk sett kan Kristin ha rukket å kjøre til Sørumsand, bryte seg inn i kårboligen, skyte ned tre mennesker, og kjøre tilbake til Oslo.

Orderud saken

- Allerede i sin andre politiforklaring hevdet Kristin at hun hadde kjørt en budrute for Aftenposten drapsnatta. Hun skal ha gjort jobben for en venn av seg. Denne vennen var ikke i bilen drapsnatta.
- Grønnerøds forsvarer sier til Dagbladet at utskriftene gir hans klient et fullstendig alibi for de kritiske timene for drapstidspunktet natt til pinseaften, og at han umulig kan ha vært på Sørumsand. Tidspunktet er for kort i de opphold i telefonsamtalene det er snakk om.

Nittedal

- Høsten 1998 ble en taxisjåfør skutt mens han satt i bilen i Nittedal.
- Den polititet mistenke nektet for å ha vært i nærheten av åstedet den kvelden.
- Men politiet kunne med utskrifter fra basestasjoner vise at han hadde vært i området.

Tele(n)(br)or ser deg

- Anta: Du får følgende brev fra politiet:
  "Vi har fått melding om uvettig og tildels livsfarlig kappkjøring på strekning Tromsø - Nordkjosbotn natt til mandag. Fra Telenor Mobil har vi fått opplyst hvilke mobiltelefoner som har vært i kontakt med Telenors basestasjoner på denne strekningen i løpet av natten. Utskriften viser at din telefon kl 02:00 var i kontakt med Telenors basestasjon ved Tromsø-brua. 35 minutter senere ble den registret i Nordkjosbotn. Vi vil gjerne at du møter på Troms Politikammer ..."

Tele(n)(br)or ser deg

- Anta: Du får følgende brev fra politiet:
  "Vi har mottatt en anmeldelse på innbrudd i varehuset Jekta natt til lørdag. Fra Telenor Mobil har vi fått opplyst hvilke mobiltelefoner som har vært i kontakt med Telenors basestasjoner rundt Jekta i løpet av natten. Utskriften viser at din telefon i tidsrommet mellom kl 01:10 – 02:40 var i kontinuerlig kontakt med alle Telenors basestasjoner i området. Vi vil gjerne at du møter på Troms Politikammer ..."

Avlyttet digitale mobilsamtaler

- USA 1997: Ved en glipp ble et krypteringdokument fra en mobiltelefonprodusent lagt ut på Internett. Nå har en student ved Berkeley klart å knekke krypteringskoden og avlyttet digitale mobilsamtaler.
- Problemet skyldes delvis NSAs restriktive krypteringspolitikk. NSA har gjennomført tiltak for å hindre at sterke krypteringsalgoritmer skal falle i urette hender.
- På sedvanlig amerikansk manér frykter nemlig NSA at terrorister skal kunne føre trådløse samtaler uten at NSA har mulighet til å avlytte dem.

Avlyttet digitale mobilsamtaler

- ”Digitale mobiltelefoner er ikke så sikre som folk gjerne vil tro,” sier Bruce Schneier i Counterpane. Sammen med kollega John Kelsey og ingeniørstudent David Wagner har han bevist at det tar bare få minutter å knekke CMEA-krypteringen på en vanlig PC.
- CMEA står for Cellular Message Encryption Algorithm og er den krypteringsalgoritmen som brukes til å sikre kontrollkanalen i de fleste amerikanske digitale mobilsystemer.

Avlyttet digitale mobilsamtaler

- Schneier understreker at den amerikanske sikkerhetsalgoritmen matematisk lett kan styrkes, men at det nok er vanskeligere å få politisk gehør for en slik endring av systemet.
- I 1997 ble f.eks. en mobilsamtale mellom kongresstalsmann Newt Gingrich og en kollega spilt inn på bånd av en privatperson. (Analog mobilsamtale)
- Den europeiske smartkortbaserte GSM-standarden ikke kan knekkes på samme måte som CMEA-systemet fordi GSM bruker en annen algoritme.

Avslått mobiltelefon kan avlyttes

- Sverige 1999: ”Med svært enkelt teknisk utstyr er det mulig å avlytte samtaler i rom der det finnes en mobiltelefon, selv om telefonen ikke er påslått.” Det hevdet sjefen for det svenske sikkerhetspolitiet, Anders Eriksson. Säpo klassifiserer derfor mobiltelefonen som en sikkerhetsrisiko.
- ”Det er rimelig enkelt å benytte mobiltelefoner til avlytting av viktige møter. Det holder med å kjenne til et telefonnummer for å kunne avlytte hva som sies i et rom,” påsto Eriksson. Han advarer på det sterkeste folk mot å ta med seg en mobiltelefon inn på viktige møter – den kan avlyttes selv om den er avslått, sa han.

Avslått mobiltelefon kan avlyttes

- Eriksson ville ikke gå inn på hvordan man går fram for å avlytte telefoner på denne måten eller hvilket teknisk utstyr som kreves for å få det til.
- Spionasje er nå i mindre målestokk enn før er rettet mot militære installasjoner men mer mot teknologi, politisk informasjon og mot økonomiske mål. Hemmelig informasjon må ikke lagres på IT-systemer. Informasjonen må heller skrives ned på papir og låses inn i en solid safe, mener han.
- ”Det er ikke bare fra øst spionene kommer, nå spionerer alle på alle,” sa Eriksson.

Avlytter rom med mobilen

- Mobiltelefoner kan misbrukes til romavlytting. Det tyske datatilsynet slår alarm om at et par håndgrep er nok for å gjøre apparater fra Nokia og Ericsson til spionmikrofoner.
- Metoden er enkel: På mobiltelefonen monteres utstyr for handsfree-samtaler. Du programmerer telefonen med «autosvar», altså at telefonen selv besvarer oppkall uten å gi fra seg ringesignal. Så etterlater du telefonen i et rom.
- Deretter kan du ringe opp eget mobilnummer og overhøre samtaler som foregår i rommet der telefonen ligger.

Avlytter rom med mobilen

- Lederen for det tyske datatilsynet, Joachim Jakob, er sjokkert over hvor enkelt det var å misbruke telefonen på denne måten. I et brev til innenriksminister Otto Schily krever han at tyske myndigheter snarest må ta opp saken med de nordiske produsentene og få satt en teknisk stopper for mulighetene til misbruk.
- - Det er Nokia og Ericssons ansvar å sikre sine produkter, sier han. (Dagbladet, 2.10.99)

ISDN

- ISDN telefoner er perfekte avlyttingsmikrofoner
- Man kan lytte på hva som skjer i nærheten av telefonen uten at røret er løftet av.
- Dette er en del av spesifikasjonen av ISDN.

Økt GSM-overvåkning

- Sept 99: Media melder om at Telenor og Netcom etter pålegg fra myndighetene vil installere utstyr som muliggjør overvåkning av mobilnettet (GSM) og opptak av samtaler.
- Begrunnelse: bedre politiets etterforskningsrutiner.

Nye vaner for kriminelle?

- I mange kriminalfilmer kan vi se hvordan de kriminelle kvitter seg med våpen og klær som kan knytte dem til åstedet. I fremtiden vil vi nok oppleve at de i tillegg også kvitter seg med mobiltelefonen og GPS-kartet.
- Flere vil nok kjøpe seg ny telefon med ringkontant når de handler inn til helgen.
- Men kanskje er det for sent – kanskje har politiet allerede sikret seg et stemmeavtrykk av samtalen nær åstedet. Eller de er fanget opp av kameraene til veivesenet, bensinstasjonen, politiet, etc.

Ny GSM tjeneste?

- Telenor burde melde fra dersom telefonen til en av de personer man ofte ringer er i nærheten.

Hackerne ser det meste

Back orifice

- 3. august ble hackerverktøyet Back Orifice (BO) sluppet av Cult of the Dead Cow (cDc).
- Trojanske hest som via nettet muliggjør overvåke og fjernstyring av en Window95/98 pc.
- Angreps metode: sende BO til offeret via en E-Mail. Når BO startes, installerer den seg selv som en "service" i den lokale arbeidsstasjonen samtidig som den gjemmer seg ved å slette den opprinnelig installasjon filen.

Back orifice

- BO gjemmer seg også for Windows95/98 og vises ikke på "Control+Alt+Delete" listen.
- Programmet har fått stor oppmerksomhet blant "hobby hackere", og i perioden 3. til 7. august ble det lastet ned 35.000 ganger. Hackerverktøy er ofte interessante for mange og noe av det som er bekymringsfullt er at BO er et meget kraftig verktøy som er relativt enkelt å bruke.

Back orifice

- En inntrenger vil blant annet kunne gjøre dette på arbeidsstasjonen til den som blir "angrepet":
  - Se hva som er på skjermen
  - Se hva som blir skrevet på tastaturet
  - Installere programvare
  - Avinstallere programvare
  - Restarte maskinen
  - Se lagrede passord

Back orifice

- Se og editere Windows registeret
- Koble opp og ned maskinen til andre nettverks servere/ressurser
- Få maskinen til å låse seg
- Inntrengeren har dermed like mange rettigheter på maskinen som offeret selv.
- Dette er ikke noe datavirus i seg selv, men kun å betraktes som fiendtlig kode. Med BO vil en fremmed bruker kunne få kontroll over en annen arbeidsstasjon.

NetBus verre enn Back Orifice?

- OSLO: Det svenske dataviruset NetBus lar uvedkommende trenge inn i datamaskinen, lese e-post og stjele brukernavn, passord og kontonummer til nettbanken.
- I oktober 1998 slo Telenor Nextel og Tele2 alarm over viruset Back Orifice. "Det er det verste virusprogrammet vi har sett til nå," sa informasjonsdirektør Arne Cartridge i Telenor Nextel.
- Som Back Orifice er NetBus både et virus og et program. Og som andre trojanske hester spres det vanligvis som e-post, eller som en skjult fil i programmer som lastes ned fra nettet.

NetBus

- NetBus kan fjernstyre andre PC-er koplet til nettet. ”Tanken var å lage et program til å erte vennene mine,” sier opphavsmannen, unge Carl-Fredrik Neitker til TT.
- NetBus er nå spredd over hele verden. Neitkers egen nettside har 1.500 – 2.000 besøk per dag.
- Det kan være morsomt å fjernstyre CD-ROMen til en kamerat. Men ikke engang Neitker synes det er moro at uvedkommende kan stjele passordet til nettbanken hans.
- Bankene hevder at verken NetBus eller Back Orifice kan manipulere kontoene, men svenskene er slett ikke overbevist om at bankene snakker sant.

Advarsel

- Disse hacker-verktøyene er laget av unge entusiaster.
- Hva kan vel ikke en organisasjon som CIA og DoD klare å lage i sine laboratorier. Det samme gjelder terroristorganisasjoner og etterretningsorganisasjoner verden over.

Virus

- *Ett virus er et selvreplikerende program som er i stand til å kopiere seg selv og som kan infisere andre program eller datasystemer.*
- Utvidet betydning også om ormer (worms) og Trojanske hester (Trojans).
  Dette er programmer som forsøker å kopiere seg selv til så mange maskiner som mulig.

Trojanske hester og ormprogrammer

- Et ormprogram er ett eller flere program som via datanettet er i stand til å spre kopier av seg selv til andre datamaskiner. Til forskjell fra virusprogrammer behøver ikke ormprogrammer å koble seg til et vertsprogram, men kan handle på egen hånd.

Trojanske hester og ormprogrammer

- En Trojansk hest er ett program som gjør ”ulovlige” operasjoner som det er meningen at brukeren ikke skal kjenne til.
- Et virus kan sees på som en type Trojanske hester.

Stealth-virus

- Stealth-virus skjuler de endringer det har foretatt i filer og bootsektor. Dette gjøres ved å overvåke de systemfunk-sjoner som anvendes til lesing av filer eller sektorer på lagringsmedia og forfalske resultatet av lesingen. Et program som forsøker å lese en infisert fil eller sektor ser kun den normale ikke-infiserte filen i stedet for den virkelige smittede varianten.
- Virusets forandringer kan snike seg unna antivirusprogram. Men dette krever at at viruset er minneresident, noe som igjen kan oppdages av antivirusprogram.
- Eks. Brain, ”Number of the Beast”, Frodo (4K)

Polymorft virus

- Ett Polymorft virus er ett virus som skaper endrede, men fungerende kopier av seg selv. Dette gjøres for å forsøke å forhindre at at antivirusprogram skal oppdage ulike varianter av viruset.
- En metode som benyttes av virus for å unngå å bli oppdaget av søkestrengbaserte antivirusprogram er at viruset krypteres seg selv med en variabel krypteringsnøkkel. Men siden disse virusene stort sett anvender samme dekrypteringskode og derved kan oppdages av søkestrengbaserte antivirusprogram, så er disse strengt tatt ikke polymorfe. Eks. Cascade.

Polymorft virus

- Polymorfe virus kan konstrueres ved å velge mellom mange ulike dekrypteringsmetoder som krever forskjellige dekrypteringsrutiner. Eks. Whale-viruset hvor kun en av disse rutinene er synlig i alle kopier av viruset. På denne måten må et søkestrengbasert antivirusprogram søke gjennom en rekke søkestrenger for å kunne oppdage et polymorft virus.
- For å unngå å bli oppdaget varierer mer avanserte polymorfe virus som f.eks. V2P6 instruksjonsrekkefølgen i kopiene.

Polymorft virus

- En av de mest sofistikere formene av polymorfe virus finner vi i "The mutation Engine" (MtE) som kommer i form av en objektmodul. Ved hjelp av MtE kan all virus gjøres polymorfe ved å legge til visse anrop til disses assembler-kildekode og linke disse till mutasjonsmotoren og til tilfeldigtalls-genererte moduler.

Første virus som angriper nettsider

- November 1998: html-kodede Internett-sider kan bli angrepet av virus. Det første html-viruset, html.internal, er en demonstrasjon, men kan være en forvarsel om fremtidige problemer.
- Tanken på et virus som kan spre seg gjennom html-kodede Internett-sider skremmer nettbransjen.
- "Det ser til sist ut som om virus-miljøet har oppdaget Internett," sier Richard Smith hos Phar Lap Software. "HTML sider er svært mobile, og er skapt for å bli sendt til folk," sier Smith, og peker på at nettsider vil være en effektiv spredningsform for virus.

Første virus som angriper nettsider

- Det første kjente HTML-viruset ble skapt av Virus Information Center. Det er skapt for å være en demonstrasjon, og skal ifølge Wired.news være rimelig harmløst. Siden viruset bare formerer seg i sidene gjør det først og fremst skade ved å fylle opp datamaskinens minne, noe som kan få maskinen til å krasje. Viruset utnytter samtidig spesiell Windows 98-programvare, og skal bare kunne formere seg hvis sidene er skrevet med VisualBasic Script.
- Ifølge Microsoft vil funksjoner i Internet Explorer 4.0 advare mot viruset

Serbisk hacker-angrep mot Kosovo

- Oslo (23.10.1998) Hackere fra den serbiske organisasjonen Crna Ruka (Sorte hånd) manipulerte natt til tirsdag nettsidene til Kosova Information Center, heter det i en melding fra senteret.
- Nettstedet til Kosova Information Center (KIC) oppdateres flere ganger i døgnet med meldinger på engelsk, tysk og albansk. Ifølge Beograd-korrespondenten Vesna Peric-Zimonjic i det internasjonale nyhetsbyrået IPS, er nettstedet en primær kilde til informasjon om hva som skjer i Kosovo.

Serbisk hacker-angrep mot Kosovo

- KIC melder at hackerne la det serbiske nasjonale symbolet på KICs åpningsside, sammen med blant annet en tekst på engelsk: "Velkommen til websiden til de største løgnerne og morderne". KIC ble gjort oppmerksom på forholdet da lesere ringte dem. Albanske studenter kontaktet webhotellet i New York som drifter siden, og fikk dem til å gjenopprette den opprinnelige siden.
- I forrige uke var websidene til den albansk-språklige avisa Zëri i Kosovës (Kosovos røst) hacket på tilsvarende måte.

Serbisk hacker-angrep mot Kosovo

- Sorte hånd er en serbisk terrororganisasjon fra før første verdenskrig. KIC mener at betegnelsen kan være et dekke for serbiske regjeringskretser, og at hackingene kan betraktes som en del av Milosevic-regimets angrep på etniskalbanske og opposisjonelle medier de siste ukene.

100 hackere klare til å sabotere Indonesia

- 1999: Jose Ramos Horta bruker hackere som trussel mot Indonesia hvis ikke folkeavstemningen går som den skal.
- Det er nobelprisvinner Jose Ramos Horta står bak advarselen,melder BBC News.
  Han sier at ca. et dusin virus er laget for å infiltrere computere i Indonesia hvis det forekommer valgfusk eller avslag etter at Øst-Timors fremtid er klar etter folkeavstemningen den 30. august.

100 hackere klare til å sabotere Indonesia

- 100 hackere fra Europa og Nord-Amerika har forberedt seg på virus-kampanjen som vil kunne påføre Indonesia økonomisk katastrofe. Målet er å infiltrere computere med kontroll over banker, finansmarkedet og militæret.
- Virusene skal kunne ødelegge Indonesias banksystem, og medføre et tap på hundrevis av millioner dollar, sier Horta.
- Trusselen om dataherverk blir fremsatt fordi Horta mener det er stor sannsynlighet for at folkeavstemningen ikke vil bli gjennomført på en rettferdig måte, men at den derimot kan vise seg å bli det fremste eksempelet på valgfusk i moderne tid.

Internet ormen

- Internet-ormens perspektiver: Hvam om det er orm-programmer som ikke er oppdaget?
- Når kontrollerte du sist prosess-tabellen, og gjenkjente du ALLE prosesser?

2-8. november 1988

Onsdag 2. november

- kl. 17:00 Orm-programmet startes opp på MIT universitetet.
- kl. 18:00 Programmet hadde spredt seg til USAs vestkyst.
- kl. 19:00 UC Berkeley er angrepet av orm-programmet.
- kl. 23.30 NASA settes i alarmberedskap.

Torsdag 3. november

- kl. 00.30 Anonym melding på Internet. I meldingen angis hvordan orm-programmet utnytter ett av sikkerhetshullene til de datamaskinene som ble angrepet (fingerd).
- kl. 03.00 Feilkorrigeringer til programmet sendmail sendes ut fra UC Berkeley.
- kl. 19.00 Feilkorrigeringer til programmet fingerd sendes ut.
- kl. 23.00 TV-selskapet CBS har orm-programmet som hovedoppslag i nyhetssendingen.

Fredag 4. november

kl. 01.00 Orm-programmet er isolert og testes på et eget datanett.

kl. 06.00 Forskere ved UC Berkeley har fullstendig identifisert de enkelte deler av orm-programmet.

kl. 12.00 Forskere ved MIT universitetet har komplett programkode til orm-programmet.

kl. 17.00 Orm-programmet presenteres på slutten av “the Berkeley Unix Workshop”.

Tirsdag 8. november

NCSC (National Computer Security Center, underlagt DoD, det amerikanske forsvarsdepartementet) har møte med bl.a. DARPA, CIA, FBI, SRI, UCB, MIT, m.fl.).

Internet ormen

- November 1988: Orm-programmet var programmert til å skaffe seg adgang til andre datamaskiner ved å omgå godkjenningsprosedyrer for så å spre kopier av seg selv til de nye datamaskinene.
- 1988: Orm-program som utnyttet svakheter i finger, sendmail, .rhosts & passord (BSD)

Internet ormen

- Stor mediaomtale:
  - "New York Times" hadde historien på førstesiden i en hel uke.
  - "Wall Street Journal" og "USA Today" hadde førstesideoppslag om orm-programmet.
  - Også god dekning av diverse nyhetsstasjoner, og var blant annet hovedoppslag hos CBS.

Internet ormen

- Jakten på orm-programmets hemmeligheter og programmets skaper(e) ble også intens.
- 5. nov 1988 kunne "New York Times" melde at orm-programmet var konstruert av Robert T. Morris, en 23 år gammel hovedfagsstudent ved Cornell University, og sønn av en av USAs fremste eksperter på datasikkerhet.
- Morris ble senere utvist fra Cornell, og idømt 3 års betinget fengsel, bot på $10.000 og 400 timers samfunnstjeneste. I tillegg måtte han betale alle advokatomkostninger (estimert til $150.000).

Hvordan virket ormen?

- Et nytt orm-program startet med å lage en liste over fjerntliggende datamaskiner som så programmet i neste omgang forsøke å få adgang til. Denne listen ble bygget opp med adresseinformasjon som var lagret lokalt på datamaskinen.
- Med utgangspunkt i denne listen var orm-programmet programmert til å forsøke og bryte seg inn i de fjerntliggende datamaskinene programmet nå hadde fått adressen til. I “forsøkene på å bryte seg inn” var orm-programmet programmert til å anvende flere teknikker.

Hvordan virket ormen?

- Programmet “forsøkte” å knekke passordet til en av brukerne på den fjerntliggende datamaskinen og på denne måten logge seg inn som en registrert bruker.
- Andre teknikker som ble prøvd var å utnytte en feil i “finger”-protokollen som returnerer tilbake informasjon om en eller flere brukere på en fjerntliggende datamaskin.
- Videre ble en feil i prosessen som håndterer elektronisk post (sendmail) på de fjerntliggende datamaskiner, “forsøkt” benyttet som bakdør.

Hvordan virket ormen?

- Samtidig med at orm-programmet var programmert til å forsøke og bryte seg inn i fjerntliggende datamaskiner, forsøkte programmet å gjette passord til brukere på den lokale datamaskinen.
- Denne prosedyren for å knekke passord (*cracksome*) opererte på flere nivåer.
  - Nivå 0 (*crack_0*) leste passordfilen på den lokale datamaskinen.

Hvordan virket ormen?

- Nivå 1 (*crack_1*) undersøkte om noen brukere anvendte passord som er trivielle å gjette. Dette er passord som i hovedsak kan gjettes på bakgrunn av informasjon lagret i passordfilen, inkludert forsøk med følgende passord:
    - nullpassord (intet passord).
    - navn på brukerkonto.
    - konkatinert passord (dvs. f.eks. “blaola” dersom navnet på brukerkontoen er “bla”).
    - fornavn (til brukeren) angitt med liten forbokstav.
    - etternavn (til brukeren) angitt med liten forbokstav.
    - reversert navn på brukerkonto (dvs. “alo” dersom navnet på brukerkontoen er “bla”).

Hvordan virket ormen?

- Nivå 2 sammenlignet passordene i passordfilen mot en liste med favorittpassord. Orm-programmets liste bestod av 432 passord. Disse var for det meste engelske ord eller vanlige egennavn.
- Dersom intet av dette nyttet, var orm-programmet programmert til å ta for seg ordlisten som var lagret lokalt (“/usr/dict/words”) og så forsøke ett ord av gangen fra denne. (Ca. 250.000 ord.) Dersom et ord var angitt med stor forbokstav i ordlisten, ble ordet også forsøkt med liten forbokstav.

Finnes det flere ormer installert?

- Et skremmende tankeeksperiment er hvordan slike orm-programmer kan utnyttes av terroristorganisasjoner, etteretningsorganisasjoner og til industri-spionasje etc.
- Dersom en gruppe av personer med tilnærmet Morris sin kompetanse ble satt på oppgaven, ville disse lett kunne realisere orm-programmer som for eksempel i en krisesituasjon ville være programmert til å kunne ta seg inn i sårbare installasjoner for så og gjøre så mye skade som mulig.

Finnes det flere ormer installert?

- Dersom tilstrekkelige midler stilles til disposisjon, er det bare fantasien som setter grenser for hva som er mulig å få til med slike orm-programmer. Kanskje finnes det allerede en armada av slike programmer der ute (og her inne) – programmer som kun venter på de rette kodeordene for å aktiviseres?

Internettet følger deg

E-post over alt

- Vi tillater uten videre at mengder av elektroniske sport etterlates på Internet.
- Oliver North ble felt fordi driftsgruppen hadde sikkerhetskopier av all hans "hemmelige" e-post korrespondanse (som han selv hadde slettet fra egen maskin).

Sexkjøpere avslørt på Internett

- Etter lekkasjen i Microsofts e-posttjeneste Hotmail er flere svenske menn nå tatt med buksene ned på Internett -- avslørt som kunder av prostituerte.
- Mens porten til Microsofts Hotmail-server var åpen, greide noen å hacke seg inn på e-postkontoen til to unge prostituerte kvinner, og legge ut deres korrespondanse på Internett. Der ble det avslørt både navn og telefonnummer til flere av deres kunder.
- E-posten ble lagt ut på en anonym hjemmeside på en amerikansk server der hvem som helst kan lese dem.

Sexkjøpere avslørt på Internett

- På hjemmesiden avsløres mange intime detaljer om dem som har sendt brevene:
  «Er en trivelig og kåt mann, gift, som trenger mer enn det jeg får hjemme», skriver en mann som har fått både sitt navn og telefonnummer lagt ut på hjemmesiden.
- Flere av mennene som skriver til jentene forteller at de er forretningsmenn som iblant besøker Stockholm, og ønsker kontakt. Personene bak hjemmesiden oppfordrer besøkende om å sende e-post og ringe mennene.

Sexkjøpere avslørt på Internett

- En direktør i en velkjent svensk mediebedrift er blant de avslørte. Han har skrevet e-post til begge jentene og skriver «Jag är seriöst intresserad utav att få franska-lektioner utav er på kontinuerlig basis. Kan ni berätta mer om era lektioner, vore bra om ni även kunde bifoga en bild utav kursplanen.»
- Ti Expressen hevdtr han at han ikke kjøper seksuelle tjenester, men at han bare har skrevet til jentene av nysgjerrighet for å se om de virkelig er prostituerte.

Sexkjøpere avslørt på Internett

- Sikkerhetshullet i Hotmail ble kjent i august 99. Microsoft, som eier Hotmail, rettet opp feilen først flere timer senere. Programfeilen lå der i mange måneder, og gjorde det mulig for brukere å logge seg på andres postbokser uten passord.
- Microsoft har lagt skylden for sikkerhetshullet på hackere, ikke på dem som har kodet sidene uten å tette sikkherhetshullene.

Doubleclick

- Når du slår opp på en web-side registreres din hjemmeadresse, og man forsøker å finne ut så mye som mulig om deg.
- Dette gjøres for at den reklamen som presenteres skal være så optimal som mulig. Det er ofte reklamen og sammensettingen av denne som tar tid når du slår opp på en hjemmeside.
- Det er merkelig at selv de mest ihuga motstandere av uadressert reklame ikke reagerer på tilsvarende fremstøt på nettet.

COOKIES or Big Brother is watching you

- Cookies er en generell mekanisme med serverforbindelser (slik som CGI skript) som kan benytte både for å lager og hente fram informasjon fra klienten.
- En server som returnerer et HTTP objkt til klienten kan også sende tilstandsinformasjon til klienten som denne lagrer, inkludert hvilke URL som denne informasjonen gjelder for. Alle fremtidige HTTP forespørsler som klienten foretar til disse URLene vil inkludere et tilstandsverdien. Tilstandsobjektet kalles en ”cookie”.

Cookies

- Cookies tillater enhver web-site å lagre informasjon om ditt besøk på din disk.
- Fordeler med ”cookie”:
  - Tilbyr adgang og tjenester basert på din ID.
  - Kan lagre brukerspesifikk informasjon på klienten som så sendes over hver gang tjeneren kontaktes, f.eks. dine preferanser ved kjøp, search.com tilbyr en liste over dine 20 beste preferanser, etc.
  - Statistikk
  - Kan gi svar på hvilke deler av et web-sted som er mest populære.

Cookies

- Ulemper:
  - Representerer en trussel mot privatlivet. Cookies kan prgrammeres til å angi ha du gjør, side for side, når du besøker et sted.
  - Cookies kan være knyttet til markedsførings-databaser som styrer reklamebilder på siden.
  - Kombindert med JavaScript kan cookies fremskaffe e-mail adr din.

Doubleclick

- Doubleclick tilbyr målrettet reklame basert på cookies. Ideen er at dersom jeg er interessert i å kjøpe en bil og du er en fotograf, så skal vi dersom vi går til samme side samtidig se hhv. En Honda og en Nikon reklame.
- Dette fungerer ved at dersom du kontakter en side som er kunde av Doubleclick, så vil siden samtidig med at den sender deg sin side også kontakte Doubleclick for oppdatering av kundedatabasen. Dersom du ikke er registrert der så sender Doubleclick deg en cookie.
- Når så cookien er på plass starter Doubleclik å logge informasjon om hvilke annonser du ser nå du besøker en side. Hver gang du henter opp en ny side så oppdateres cookien med URL og/eller reklame.

Doubleclick

- Dersom du allerede har besøkt siden, så vil Doubleclick kjenne igjen cookien og basert på informasjonen i cookien sende en skreddersydd reklame til den siden du er på.
- MEN dersom du f.eks. Kikket på en side som reklamerte for en AIDS konferanse hvorpå du deretter over nettet kjøpte en flybillett til den byen hvor konferansen gikk, og disse to bitene ble solgt til et forsikringsselskap, så ble kanskje dine forsikringer sagt opp.

Cadsoft

- Cadsoft tilbød et gratis demoprogram.
- Programmet gjennomsøkte disken for ulovlige kopier.
- Dersom en kopi ble oppdaget ble brukeren invitert til å skrive ut og sende inn et skjema som ville gi ham en gratis håndbok. 400 svarte.
- I retur mottok de et brev fra firmaets advokater som bad om ca DM 6000 fra hver
- Bl.a. ansatte hos IBM, Philips & tyske mynd.

Continental Cabelvision, Hartford

- Seere ble tilbudt gratis t-shirt under visning av Holyfield-Bowe kampen 14.11.92.
- Tilbudet og telefonnr. ble bare sett av de som anvendte ulovlige dekodere.
- 140 personer ringte 800-nummeret få minutter etter annonseringen
- Gratis t-shirt pluss krav om $2000 ble sendt rekommandert til hver av dem

Continental Cabelvision, Hartford

- Oslo (14.10.1998) Microsoft-selskapet WebTV bruker et system som kartlegger informasjon om hver av de rundt 450.000 brukerne. Dette blir gjort for at annonsører skal kunne målrette annonseringen.
- I USA har WebTV rundt 450.000 brukere, og teknologien er under utprøving i Storbritannia. Hver natt oppdateres informasjonen fra TV-surferne, og verdifulle data for annonsører blir sendt videre. Hva seerne har sett og hvor brukerne har vært, hvor de har klikket samt nettvanene blir oppdatert i den sentrale basen til Microsoft-selskapet WebTV, skriver Inter@ctive Week Online.

Continental Cabelvision, Hartford

- Informasjonen i basen, som kan bli brutt ned på postnummer og demografiske data, blir tilbudt annonsører, og kan etter hvert representere en inntektskilde for Microsoft. Ifølge presidenten i WebTV, Steve Pearlman, finnes det en hel avdeling som jobber med denne informasjonen i WebTV.
- ”Hvis noen ser på en bilreklame, kan vi sende dem til nærmeste bilforhandler. Balansen er å gi nyttig informasjon til annonsører samtidig som man beskytter brukerne,” uttalte Pearlman til Inter@ctive Week Online.

Continental Cabelvision, Hartford

- Pearlman uttalte at brukerne i løpet av neste år vil få muligheten til å skru av og på individuell overvåkning når de vil, slik at annonsører kan sende annonser direkte til husholdninger.
- ”Dette er som å ha et kamera rettet mot seg 24 timer i døgnet,” sier Tom Rheinlander i Forrester Research Inc. til Inter@ctive Week Online.
- I dag informeres brukerne av WebTV om overvåkningen men uten å få muligheten til å slå av kartleggingen, ifølge ZDNet. Etter planen skal WebTV lanseres i Norge i desember neste år. (digi.no, 14.10.98)

Vandaler

- "Vandals" er en ny fellesbetegnelse på fiendtlig kode. Dette kan være kode i Java Applets, Active X, plugins, vedlegg osv, som ikke laget for å spre seg.
- Vandals kan ses på som "hit and run" og er laget for å forårsake ødeleggelser inne i infrastrukturen, stjele informasjoner og eller penger.

Vandaler

- Internet er lite regulert med hensyn til sikkerhet og det er derfor fullt mulig å benytte Vandals til å skade en spesiell organisasjon eller brukergrupper.
- Vi har ingen garanti for at virussøkere oppdager slike programmer eller plug-ins. Siden brannmurer stopper aktivitet utenfra, mens vandaler startes opp innefra, er disse heller ikke effektive.

Kanadisk webtjener

- En webtjener i Canada tilbød gratis pornofilmer. For å benytte denne tjenesten måtte brukeren hente ned en spesiell "plug-in" til sin nettleser (Netscape). Når dette var gjort lukket applikasjonen modemet for brukeren og i bakgrunn ringte et nummer 1-900 - et telefonnummer hvor man belastet brukeren pr telefonsamtale + $ 5 i minuttet. AT&T har måttet refundere $ 2.74 mill til 38.000 brukere. Caos Computer Club gjorde noe tilsvarende mot National Scottish Bank i mai 1997.

Hoax (luremail, falske advarsler)

Du klarer ikke å gjemme deg for disse!

Luremail/Advarselmail (Hoax)

- Motivet bak luremail (Hoax) er som oftes å skade eller lure offrene. Mailene sendes i beste mening ofte videre av uskyldige brukere.

Disneyworld hoax

- Kjedebrev som utgir seg for å komme fra Bill Gates. (Ikke virus)

  Subject: This is NOT a joke!! Read NOW!!
  Disney message & $5,000.00

  If you read below you will see the note from Walt Disney Jr. & Management at Disney World. Basically if this messages reaches 13,000 people, everyone will receive $5,000.00 or a free, all expenses paid, trip to Disney World in anytime during the summer of 1999.

  See the note below - its worth it!!!!

  Everyone is to resend to 15 individuals. Please read and forward to as many friends as possible ... we've checked up on this and this is no joke of a chain letter or something if this reaches 13,000 people ... duplicate entries don't count, though...So, please help & pass on ... thank you, and here you go!!!

WALT DISNEY JR. GREETING

Hello Disney fans,
And thank you for signing up for Bill Gates' Beta Email Tracking. My name is Walt Disney Jr. Here at Disney we are working with Microsoft which has just compiled an e-mail tracing program that tracks everyone to whom this message is forwarded to. It does this through an unique IP (Internet Protocol) address log book database. We are experimenting with this and need your help.

Forward this to everyone you know and if it reaches 13,000 people, 1,300 of the people on the list will receive $5,000, and the rest will receive a free trip for two to Disney World for one week during the summer of 1999 at our expense. Enjoy.

Note: Duplicate entries will not be counted. You will be notified by email with further instructions once this email has reached 13,000 people.

Your friends,
Walt Disney Jr., Disney, Bill Gates, & The Microsoft Development Team.

Open:Very Cool! hoax

- Advarsel om ett ikkeeksisterende virus med fantastisk styrke.

  THERE IS A VIRUS GOING AROUND CALLED THE A.I.D.S VIRUS. IT WILL ATTACH ITSELF INSIDE YOUR COMPUTER AND EAT AWAY AT YOUR MEMORY THIS MEMORY IS IRREPLACEABLE. THEN WHEN IT'S FINISHED WITH MEMORY IT INFECTS YOUR MOUSE OR POINTING DEVICE. THEN IT GOES TO YOUR KEY BOARD AND THE LETTERS YOU TYPE WILL NOT REGISTER ON SCREEN. BEFORE IT SELF TERMINATES IT EATS 5MB OF HARD DRIVE SPACE AND WILL DELETE ALL PROGRAMS ON IT AND IT CAN SHUT DOWN ANY 8 BIT TO 16 BIT SOUND CARDS RENDERING YOUR SPEAKERS USELESS. IT WILL COME IN E-MAIL CALLED "OPEN:VERY COOL! :) DELETE IT RIGHT AWAY. THIS VIRUS WILL BASICLY RENDER YOUR COMPUTER USELESS. YOU MUST PASS

  THIS ON QUICKLY AND TO AS MANY PEOPLE AS POSSLE!!!!! YOU MUST

AOL4FREE.COM luremail og Trojan

- Først ble luremailen (AOL4FREE) utsendt i begynnelsen av mars 1997. Så ble en Trojan med samme navn distribuert i midten av april 1997. Her kommer (AOL4FREE):

  Anyone who recieves this must send it to as many people as you can. It is essential that this problem be reconciled as soon as possible.
  A few hours ago, I opened an E-mail that had the subject heading of aol4free.com

  Within seconds of opening it, a window appeared and began to display my files that were being deleted. I immediately shut down my computer, but it was too late. This virus wiped me out.

  It ate the Anti-Virus Software that comes with the Windows '95 Program along with F-Prot AVS. Neither was able to detect it. Please be careful and send this to as many people as possible, so maybe this new virus can be eliminated.

AOL4FREE.COM luremail og Trojan

- I midten av april 1997 ble en trojan med følgende kode (sletter innholdet av C:) distribuert:

  ```
  C:
  CD\
  DELTREE/y *.*
  ```

- Her forsøkte hackere å utnytte de dementier som var kommet fra antivirusaktører i kjølvannet av AOL4FREE. Man hadde brukt samme navn (AOL4FRE.COM) og skrevet en ny Trojan.

Cancer chain letter

- Dette er kjedebrev som har fått stor spredning, og som finnes i mange utgaver. Brevene er falske og kommer ikke fra noen av de kjente kreftforeningene. Merk at e-post adressen ACS@AOL.COM eksisterer ikke.
- Eksempel 1:
  Please forward this message to EVERYONE you know. The American Cancer Society gets 3 cents every time this message is forwarded. Please make sure that you cc: American Cancer Society...(ACS@AOL.COM)

Cancer chain letter (Eksempel 2)

- Subject: This is not a chain! It could save a little girls life!
  o.k. you guys..... this isn't a chain letter, but a choice for all of us to save a little girl that's dieing of a serious and fatal form of cancer. please send this to everyone you know...or don't know at that. this little girl has 6 months left to live her life, and as her dieing wish, she wanted to send a chain letter telling everyone to live their life to fullest, since she never will. she'll never make it to prom, graduate from high school, of get married and have a family of her own. but by you sending this to as many people as possible, you can give her and her family a little hope, because with every name that this is semnt to, the american cancer society will donate 3 cents per name to her treatment and recovery plan. one guy sent this th 500 people !!!! so, i know that we can send it to at least 5 or 6.
  come on you guys.... and if you're too damn selfish to waste 10-15 minutes and scrolling this and forwarding it to EVERYONE, than one: you're one sick bastard, and two: just think it could be you one day....and it's not even your $money$, just your time. i know that ya'll will impress me !!!! i love ya'll !!!!!
  peace- Sarah "X"

Cancer chain letter (Eksempel 3)

LITTLE JESSICA MYDEK IS SEVEN YEARS OLD AND IS SUFFERING FROM AN ACUTE AND VERY RARE CASE OF CEREBRAL CARCINOMA. THIS CONDITION CAUSES SEVERE MALIGNANT BRAIN TUMORS AND IS A TERMINAL ILLNESS. THE DOCTORS HAVE GIVEN HER SIX MONTHS TO LIVE.

AS PART OF HER DYING WISH, SHE WANTED TO START A CHAIN LETTER TO INFORM PEOPLE OF THIS CONDITION AND TO SEND PEOPLE THE MESSAGE TO LIVE LIFE TO THE FULLEST AND ENJOY EVERY MOMENT, A CHANCE THAT SHE WILL NEVER HAVE. FURTHERMORE, THE AMERICAN CANCER SOCIETY AND SEVERAL CORPORATE SPONSORS HAVE AGREED TO DONATE THREE CENTS TOWARD CONTINUING CANCER RESEARCH FOR EVERY NEW PERSON THAT GETS FORWARDED THIS MESSAGE.
PLEASE GIVE JESSICA AND ALL CANCER VICTIMS A CHANCE.

IF THERE ARE ANY QUESTIONS, SEND THEM TO THE AMERICAN CANCER SOCIETY AT ACS@AOL.COM

Pass på utskriftene!

- En sann historie fra Tromsø anno 1995:
- Da ektemannen fikk mobiltelefonregningen for sin mobiltelefon (som konen lånte av og til) oppdaget han en rekke oppringninger til et for ham ukjent nummer.
- Etter litt detektivarbeid og skygging av konen kom det hele for en dag: konen hadde innledet et forhold til en av hennes mannlige arbeidskolleger
- Konen nektet først, men måtte gi tapt for mannens beviser

Naboene ser mer enn du tror!
Sonys «kikker-kamera» er populært

- 1998: Salget av det feilproduserte Sony-kameraet går strålende. Men menneskerettighetsgrupper reagere kraftig på det infrarøde kameraet som kan brukes til å filme gjennom klær.
- Det infrarøde kameraet som ser igjennom klær har fått innbyggerne i Hong Kong til å strømme til forretningene for å få tak i sensasjonen, skriver AFP. I alt 9000 Sonykameraer av den omstridte typen er sendt til Hong Kong, og ingen av dem vil bli trukket tilbake.

Naboene ser mer enn du tror!
Sonys «kikker-kamera» er populært

- Dette har fått snuskete kikkere til å starte en intens jakt for å sikre seg et eksemplar av det avslørende kameraet Sony har feilprodusert og eksportert til hele verden.
- ”En aldrende, sleip mann kom inn her i morges. Han sa han ville ha det kameraet,” forteller butikkmedarbeider i en av Hong Kongs elektro-forretninger, Lin Wa-kin.
- Dette Handycam-kameraet har en infrarød teknologi som gjør det mulig å filme i mørket. Men når et kamera med slikt spesialfilter brukes i dagslys kan det filme gjennom klær.

Naboene ser mer enn du tror!
Sonys «kikker-kamera» er populært

- Nå reagerer menneskerettighetsgruppen Human Rights Monitor på det merkelige kameraet. De sier at dersom det blir brukt til å filme noen uten av de vet om det, vil vedkommende bli anmeldt for krenkelse av privatlivet og sextrakassering.
- Etter at denne ekstrafunksjonen ble kjent, har Sony nå utviklet en ny utgave av kameraet. Dette inneholder den samme nightshot-funksjonen, men den er kun mulig å bruke i mørket. Nå håper Sony at forretningene velger å selge dette produktet i steden for den sleipe utgaven.

Tilbake til videokameraene på Oslo S

- Oslo 1998: Videokameraer finnes overalt. De kan ennå ikke sveipe over en T-baneperrong, på et blunk gjenkjenne alle som står der og automatisk videresende varsler. Men det kommer om få år.
- Algoritmisk overvåkning: overvåkningssystemer med avansert integrert mønstergjenkjenning som greier å identifisere ansikter, bilmodeller, nummerskilter på biler, og så videre.

Tilbake til videokameraene på Oslo S

- Aansiktsgjenkjennende videoovervåkning vil være en realitet om få år. Et amerikansk selskap har allerede prøvekjørt i London et program som kan sveipe over folkemengder og sammenlikne ansikter mot en portrettdatabase.
- Et viktig utviklingsområde i dag gjelder bilskiltlesende systemer for trafikkontroll. Disse kan overflødiggjøre elektroniske brikker i bomsystemer.

Tilbake til videokameraene på Oslo S

- Dessverre kan legitime sikkerhetsbehov bidra til å utvikle landsomfattende infrastrukturer for allmenn overvåkning.
  - undertrykkende regimer kjøper overraskende mange trafikkontroll-systemer.
    - Kinesiske myndigheter brukte trafikkovervåknings-systemet på Tienanmen-plassen i juni 1989 til å registrere ansikter og identifisere aktivister. Bilder som ble brukt i tv-etterlysninger for å bringe aktivister ut av dekning, bygget på disse trafikkopptakene.

Tilbake til videokameraene på Oslo S

- Den tibetanske hovedstaden Lhasa er utstyrt med et avansert trafikkovervåkningssystem, selv om det ikke har noe egentlig trafikkproblem.
- En ting er et system som utløser en alarm straks en etterlyst raner går inn i et banklokale. Tilsynelatende er et system som systematisk identifiserer og registrerer bevegelsene til opposisjonelle noe helt annet. Men her er teknologien så lik at den eneste forskjellen er brukerens demokratiske sinnelag.

Tilbake til videokameraene på Oslo S

- Oslo S i 2001: 500 videokameraer ser det mest av aktiviteten. V hj a algoritmisk overvåkning følges alle uønskede personer bevegelser.
- Etter at kameraene har identifisert de uønskede personene så følges disse også av stasjonens retningsstyrte mikrofoner.

Modellmakt

- Professor Stein Bråthen ved UiO lanserte for mange år siden sin modell-makt teori om at avstanden mellom de som behersket modellene og de som ikke gjorde var voksende.
- Dette gjelder vel til full i dag hvor vi har vi blant gruppen med lavest utdannelse finner mange "teknologiske analfabeter".

Avslutning

- Vi legger vel alle igjen tilstrekkelig med spor s.a. det meste av vår aktivitet kan etterspores -- og, vi tenker ikke på det.
- Vi trenger en offentlig debatt om teknologiens utvikling og skyggesider.

Linker

- NetBus:
  www.atremo.se/virus/beskrivning/netbus.htm
- BackOrifice:
  www.atremo.se/virus/beskrivning/back_orifice.htm
- Allmänt om virus:
  www.atremo.se