

UiO : Institutt for informatikk

Hvordan hackes vi?

IN1020 – Introduksjon til datateknologi
19.10.2023

Kristin Skar
kritisk@ifi.uio.no

Datateknologi og sikkerhet

Tema for tema:

1. Datasikkerhet - Er det så viktig? (27.sept)
2. Hvem er hvem på internett? Hvordan kunne stole på digitale aktører (28.sept)
3. Kryptografi – nøkkelen til (fungerende) digital samhandling (12.okt)
4. **Hvordan hackes vi? (19.okt)**
5. Å skape trygge digitale tjenester krever innsats (25.okt)

I dag: Hvordan hackes vi?

Ressurser:

- Forelesning 19.10.23
- Tre temavideoer:
  - 08 – Angrepsvektor og skadevare
  - 09 – Sikre datasystemer
  - 10 – Sikkerhetskultur og sosial manipulasjon
- Ukeoppgaver og pensumlitteratur (Kap. 5 (115-123), 7 (169-182 + 189-195), 15 (377 -389))

Nøkkelord:

- Systemsikkerhet
- Applikasjonssikkerhet
- Sosial manipulasjon

Definisjoner

Digital sårbarhet: En feil i et IKT-system som kan utnyttes.

Skadevare: Samlebetegnelse på programvare som har som mål å gjøre skade.

Angrepsvektor: Metoden en angriper bruker for å utføre et angrep på en datamaskin, et nettverk eller et datasystem

Hckere er (stort sett) ute etter:

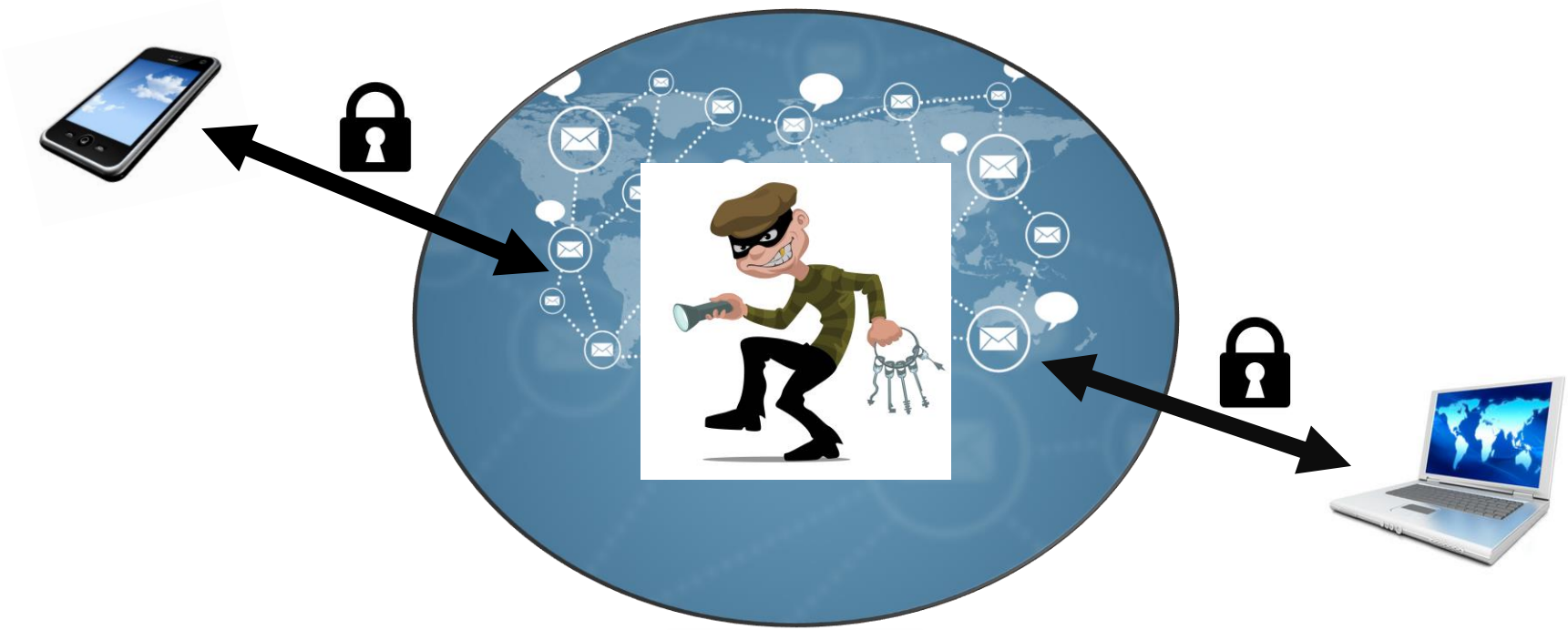
Hva:

- Tilgang til informasjon
- Endre/forfalske informasjon
- Utilgjengeliggjøre informasjon

Hvordan:

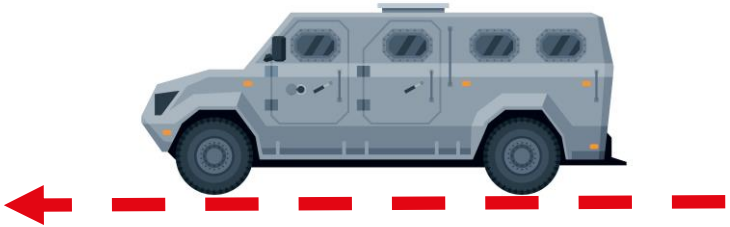
- ID-tyveri
- Utnytte sårbarheter i programvare
- Få noen til å gi deg det du vil ha

Tradisjonell sikkerhetsmodell:
Stoler på endesystemene, nettverket anses upålitelig.



Systemsikkerhet







«Å bruke kryptering på internett tilsvarer å bruke en pansret bil for å levere kredittkortinformasjon fra en som bor i en pappkartong til en som bor på en parkbenk»

Gene Spafford – «Spaf»

Programvare:

Applikasjonsprogramvare:

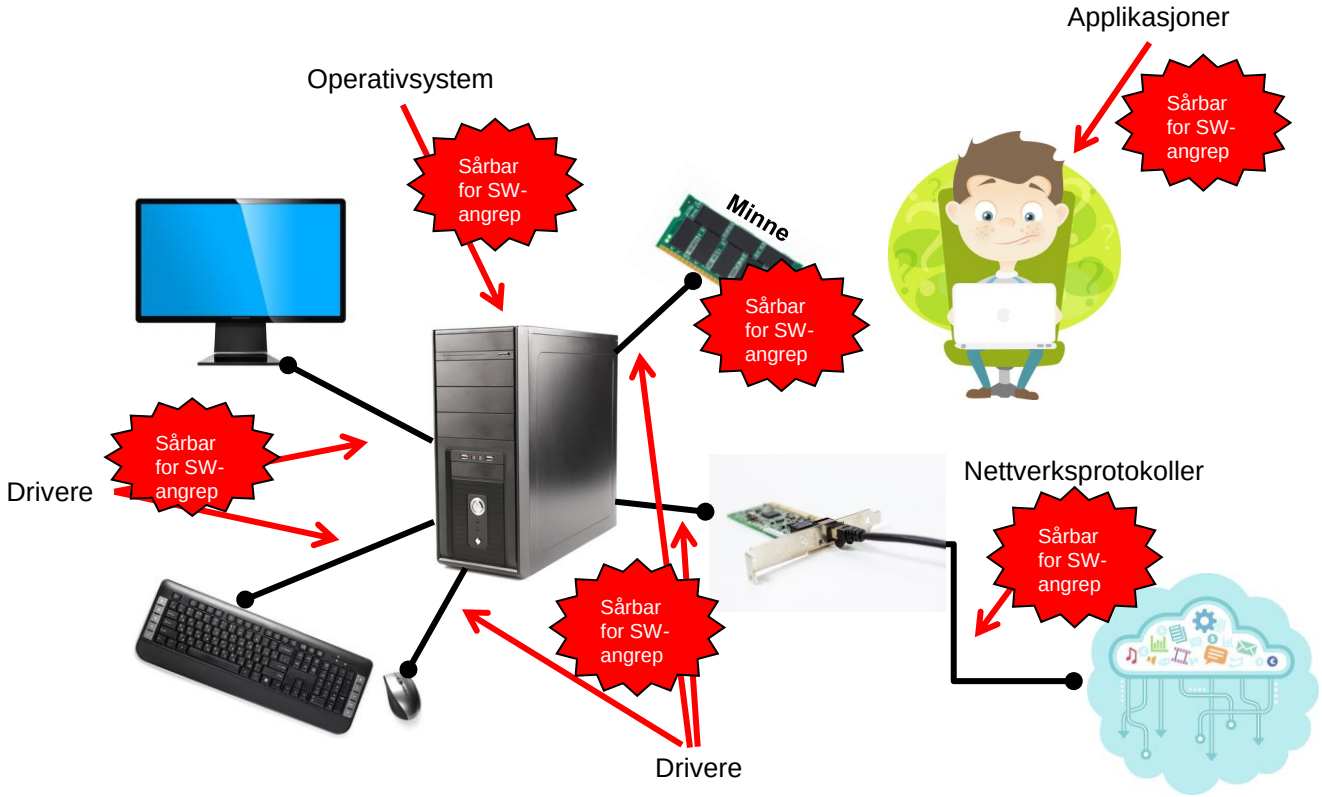


Applikasjonssikkerhet

Systemprogramvare:



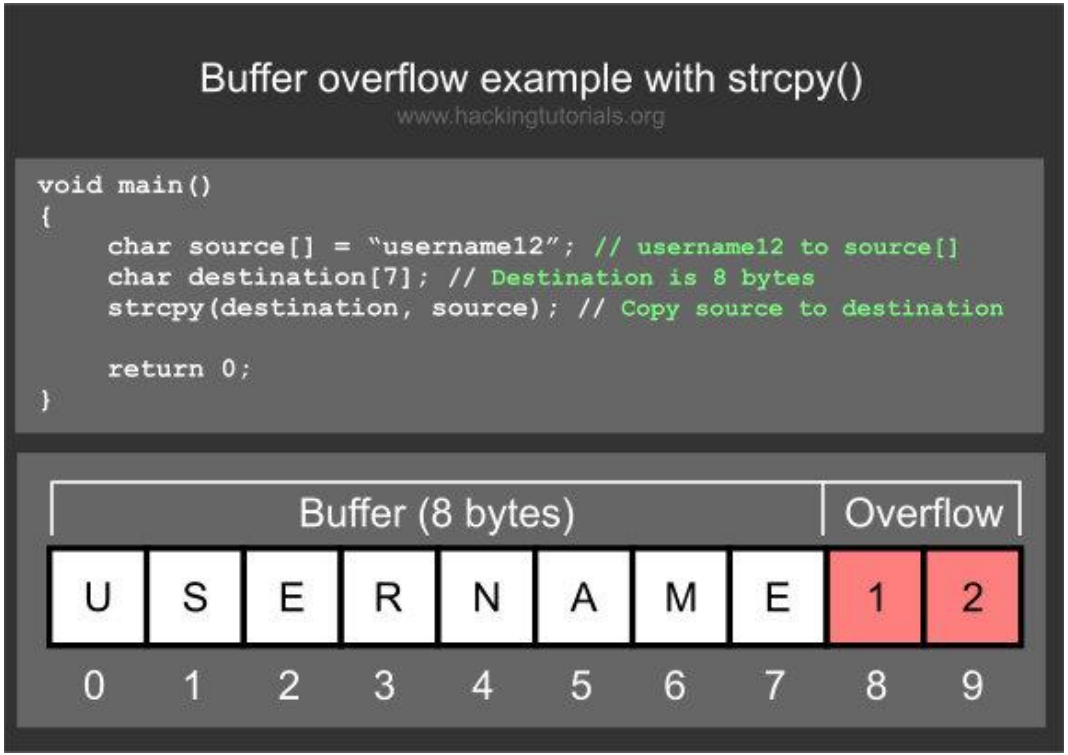
Systemsikkerhet


Applikasjoner
Operativsystem
Sårbar for SW-angrep
Sårbar for SW-angrep
Minne
Sårbar for SW-angrep
Sårbar for SW-angrep
Drivere
Nettverksprotokoller
Sårbar for SW-angrep
Sårbar for SW-angrep
Drivere

Kan man «hacke» minnet i en datamaskin?



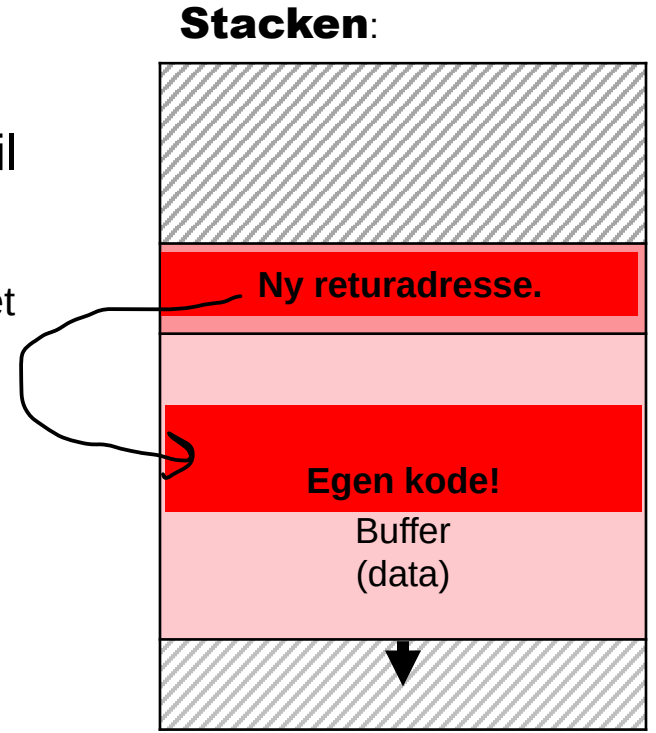
Et buffer er en sammenhengende seksjon i minnet i datamaskinen, avsatt til å inneholde data.



Kan dette brukes kreativt?

- JA – gjennom å kjøre slike sårbare programmer *kan* man skrive uhemmet til minnet i datamaskinen:
  1. Plassere egen programkode på steder i minnet hvor det ligger *kjørbar kode.*
  2. Endre en funksjons returadresse til å isteden peke til adressen i minnet der din kjørbare kode er plassert.

➢ For den interesserte (Computerphile): https://www.youtube.com/watch?v=1S0aBV-Waeo



Kan det være skadelig?



JA - brukes aktivt av hackere:

- Kan klare å kjøre egen programkode
- Kan starte andre programmer enn tiltenkt

Kan applikasjoner «hackes»?



Kjennetegn ved applikasjoner

Svært ofte:

- Dialog med bruker(e)
- Behandler input fra bruker(e)
- I bakkant av applikasjonen benyttes en *database* for lagring av informasjon.

SQL injisering

Eksempel: Tabellen «Bruker»:

BrukerId	Brukernavn	Passord	Fornavn	Etternavn	Kredittkort #
1001	anneh	ewtgfst45yh	Anne	Hansen	1609983275417533
1002	pederaa	67efg3ndfa	Peder	Aas	4586890148239766

Eksempel på brukerdialog:

Oppgi brukernavn: anneh Oppgi passord: xyxyxy OR 1=1

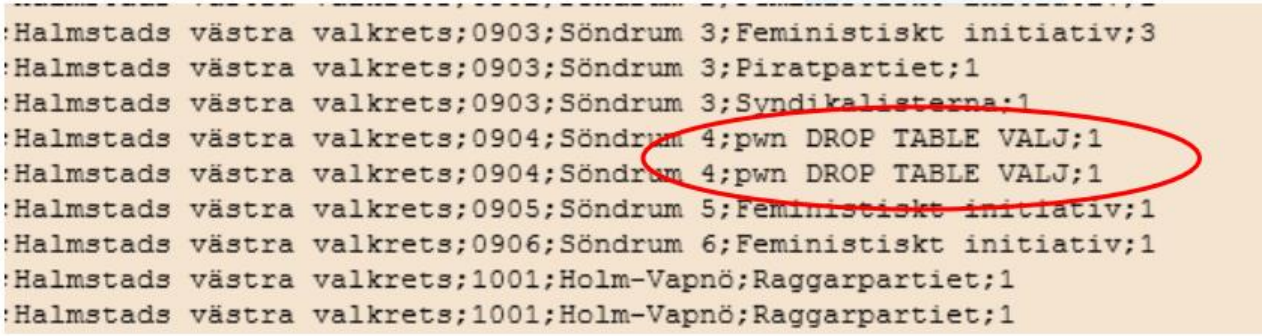
Dette kan resultere i følgende gyldige SQL-setning:

```
SELECT * FROM Bruker
WHERE Brukernavn = anneh and Passord = xyxyxy  OR 1=1;
```

- For den interesserte (Computerphile): https://www.youtube.com/watch?v=ciNHn38EyRc

Svensk valgsabotasje ☺

«Hacking swedish election with pen and paper»:



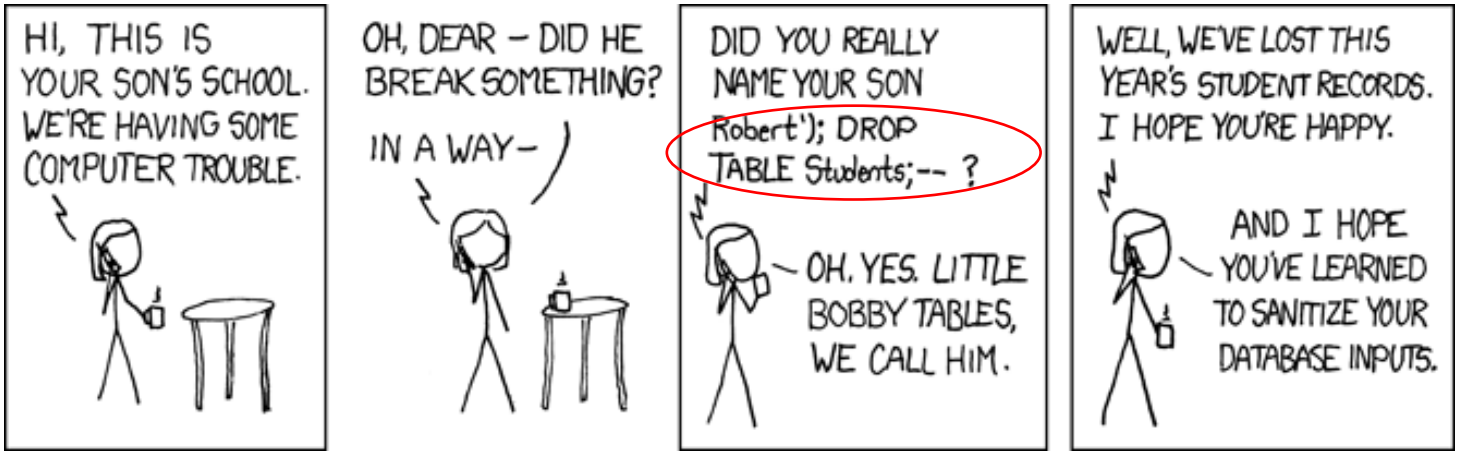
```
:Halmstads västra valkrets;0903;Söndrum 3;Feministiskt initiativ;3
:Halmstads västra valkrets;0903;Söndrum 3;Piratpartiet;1
:Halmstads västra valkrets;0903;Söndrum 3;Syndikalisterna;1
:Halmstads västra valkrets;0904;Söndrum 4;pwn DROP TABLE VALJ;1
:Halmstads västra valkrets;0904;Söndrum 4;pwn DROP TABLE VALJ;1
:Halmstads västra valkrets;0905;Söndrum 5;Feministiskt initiativ;1
:Halmstads västra valkrets;0906;Söndrum 6;Feministiskt initiativ;1
:Halmstads västra valkrets;1001;Holm-Vapnö;Raggarpartiet;1
:Halmstads västra valkrets;1001;Holm-Vapnö;Raggarpartiet;1
```

Forsøk på sabotasje ved å slette data/tabeller:

SELECT * FROM Brukere WHERE Brukernavn = anneh; DROP TABLE Valg;

- Mer info: https://www.wired.co.uk/article/sweden-election-hack

Nerde-humor: «Exploits of a Mom»



Kilde: https://xkcd.com/327/

Cross Site Scripting (XSS)



1. Angriper plasserer ondsinnede kode på en webside, kamuflert som innhold fra en bruker. Lagres på web-tjeneren.



2. Intetanende bruker besøker websiden, og ondsinnet kode sendes tilbake til brukeren med innholdet.

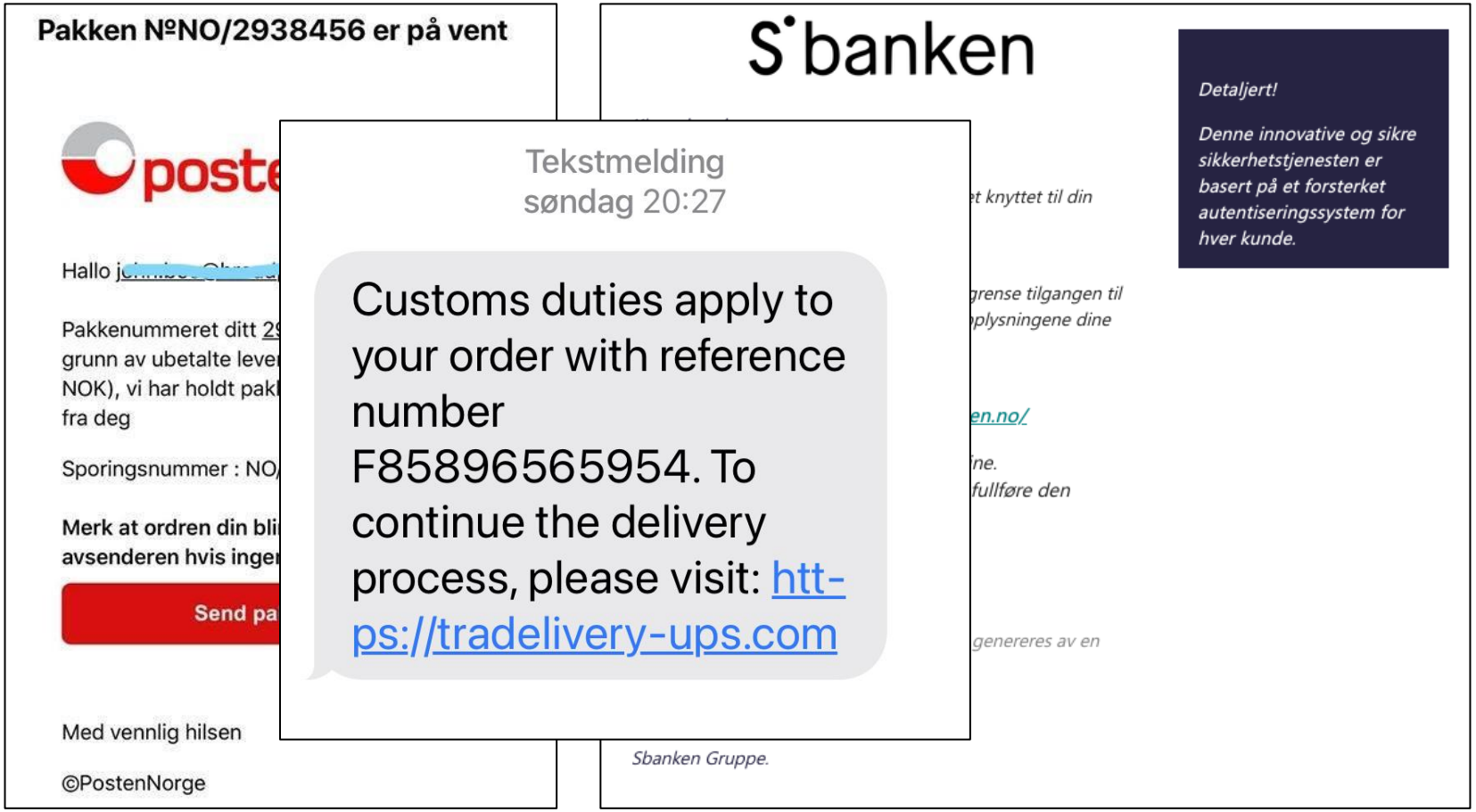


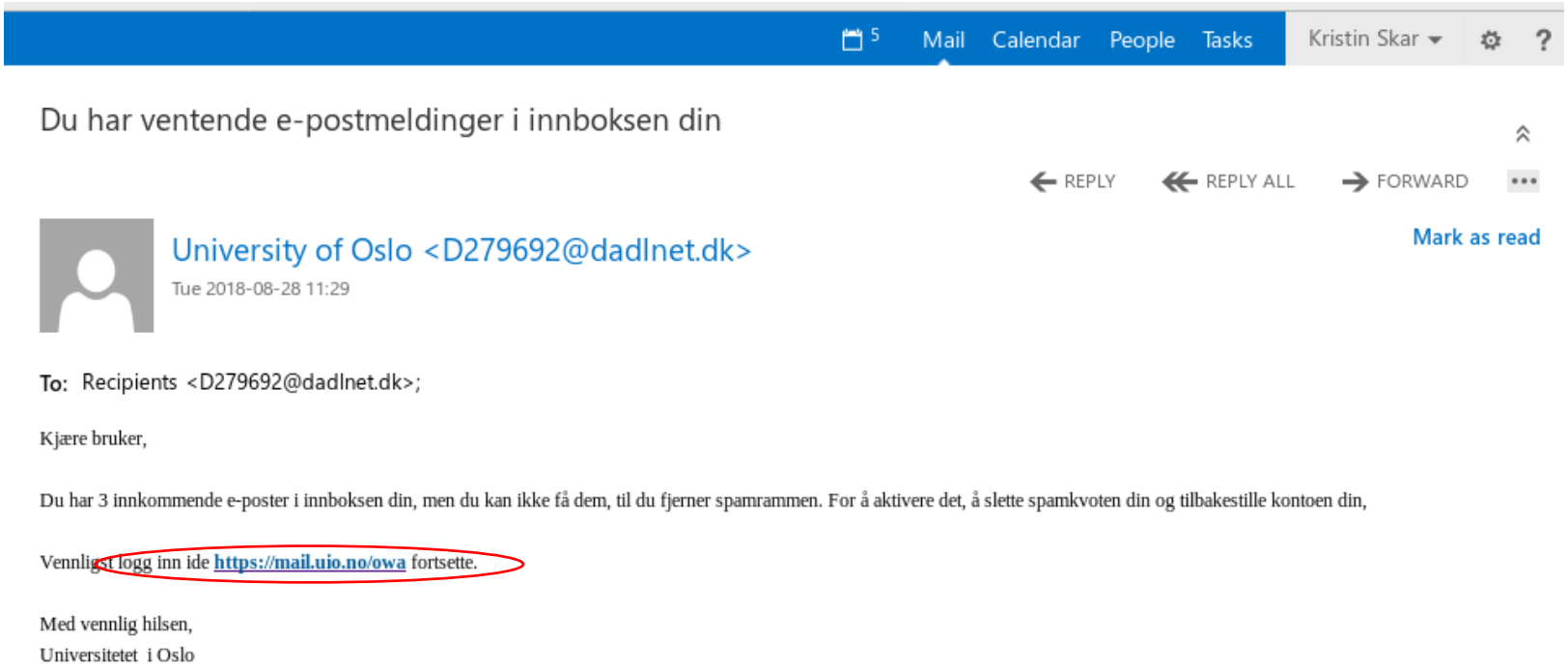
3. Angriperen tar kontroll over brukerens maskin og/eller data via den injiserte koden.

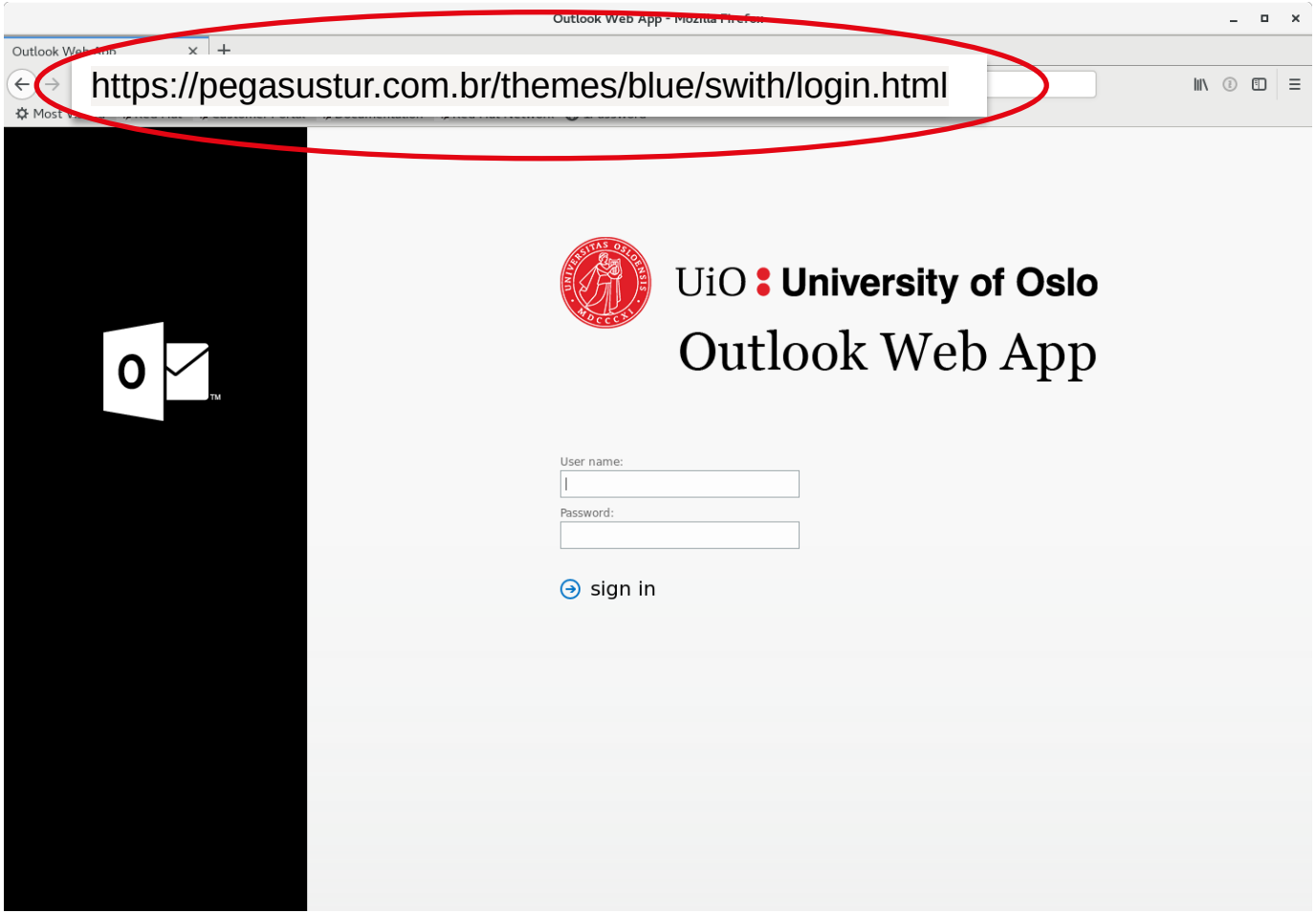
- For den interesserte (Computerphile): https://www.youtube.com/watch?v=T1QEs3mdJoc

Utgjør du og jeg en trussel?




Pakken NºNO/2938456 er på vent
Hallo j
Pakkenummeret ditt 2
grunn av ubetalte leve
NOK), vi har holdt pak
fra deg
Sporingsnummer : NO
Merk at ordren din bli
avsenderen hvis inge
Send pa
Med vennlig hilsen
©PostenNorge
Tekstmelding
søndag 20:27
Customs duties apply to your order with reference number F85896565954. To continue the delivery process, please visit: htt-ps://tradelivery-ups.com
S banken
Detaljert!
Denne innovative og sikre sikkerhetstjenesten er basert på et forsterket autentiseringssystem for hver kunde.
et knyttet til din
grense tilgangen til
plysningene dine
en.no/
ine.
fullføre den
genereres av en
Sbanken Gruppe.


5 Mail Calendar People Tasks Kristin Skar
Du har ventende e-postmeldinger i innboksen din
REPLY REPLY ALL FORWARD
Mark as read
University of Oslo <D279692@dadlnet.dk>
Tue 2018-08-28 11:29
To: Recipients <D279692@dadlnet.dk>;
Kjære bruker,
Du har 3 innkommende e-poster i innboksen din, men du kan ikke få dem, til du fjerner spamrammen. For å aktivere det, å slette spamkvoten din og tilbakestille kontoen din,
Vennligst logg inn ide https://mail.uio.no/owa fortsette.
Med vennlig hilsen,
Universitetet i Oslo


https://pegasustur.com.br/themes/blue/swith/login.html
UiO : University of Oslo
Outlook Web App
User name:
Password:
sign in

Bedragere lurte ansatt til å utbetale en halv milliard kroner

- Oslo-politiet har samarbeidet med FBI
- Ingen pågrepet så langt

VG, 18.04.2016

nrk.no, 19.12.2019

UiT svindlet for 12 millioner

UiT betalte ut 12 millioner kroner til det som viste seg å være svindel. Pengene gikk til det som så ut som en faktura for en røntgenmaskin.

Nordlys, 21.05.2020

UiT advarer mot falsk e-post med virusinfisert vedlegg

Utenlandske «direktørsvindlere» stjal 770.000 kroner fra festspillene i Nord-Norge

Med falske epostadresser og god norsk klarte svindlere å få festspillene i Nord-Norge til å overføre store summer til kontoer i England og Tyrkia.

NTB
Publisert: 20.09.2017 – 06:38 Oppdatert: 20.09.2017 – 07:33

DN, 20.09.2017

Er jeg en “sårbarhet”?

JA!

Men; Du er også en viktig forsvarsmekanisme.



Mennesker utnyttes – også digitalt

- Offer for svindelangrep
- Utpressing/overtalelser

«Sikkerhetskultur»

(God eller dårlig?)

Vanskeligere og vanskeligere å ikke la seg lure.

Deepfakes utnytter kunstig intelligens for å lage videoer og lydinnhold det er svært vanskelig å avsløre som falskt.



Sup



DNS og sikkerhet – og et eksempel på en utnyttelse

- DNS: Navneoppslag, knytter *maskinnavn* til IP-adresse:
  - devilry.ifi.uio.no -> 129.240.65.20
  - En maskin forespør typisk en *navnetjener* om adresse.
  - Kommunikasjonen foregår i klartekst
- Fallgruver:
  - DNS-forfalskning: Uvedkommende introduserer uriktige opplysninger i navnetjener
  - DNS-modifisering: Man in the Middle-angrep, forfalsker meldinger
  - DNS-kapring: Endre hvilke navnetjener offerets maskin benytter

➢ Stol aldri ubegrenset på et *domenenavn*. Vanskelig å oppdage feil.

Kan maskinvare «hackes»?



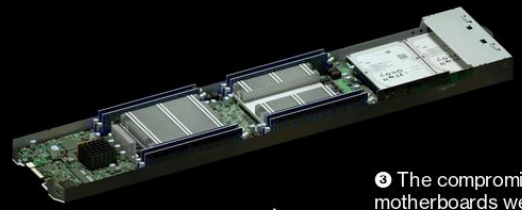
How the Hack Worked, According to U.S. Officials

❶ A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.



❷ The microchips were inserted at Chinese factories that supplied Supermicro, one of the world's biggest sellers of server motherboards.



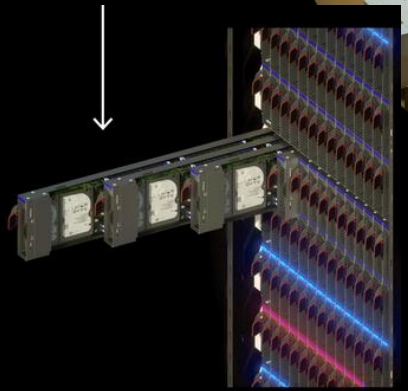


❸ The compromised motherboards were built into servers assembled by Supermicro.

❹ The sabotaged servers made their way inside data centers operated by dozens of companies.



❺ When a server was installed and switched on, the microchip altered the operating system's core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.



Kan vi stole på leverandørkjeden?

Kilde:
https://www.digi.no/artikler/kina-kan-ha-infiltrert-nettverket-til-naermere-30-amerikanske-selskaper/447913

Læringsmål

- Kjenne til sårbarheter knyttet til *systemprogramvare*.
- Kjenne *applikasjonssikkerhet*, og vanlige sårbarheter i applikasjoner.
- Mennesket som reell sårbarhet.
- Angrepsvektor og sikre *datasystemer*:
  - Hva skal til for at vi skal kunne stole på datasystemet
  - Ingenting er sikrere enn det svakeste ledd.

Takk for i dag!

mn.uio.no/ifi

