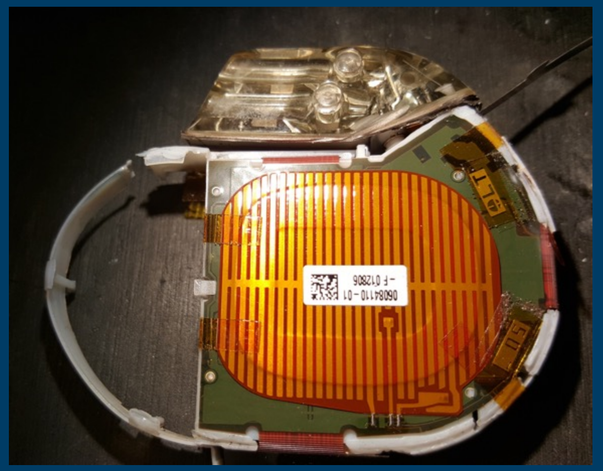
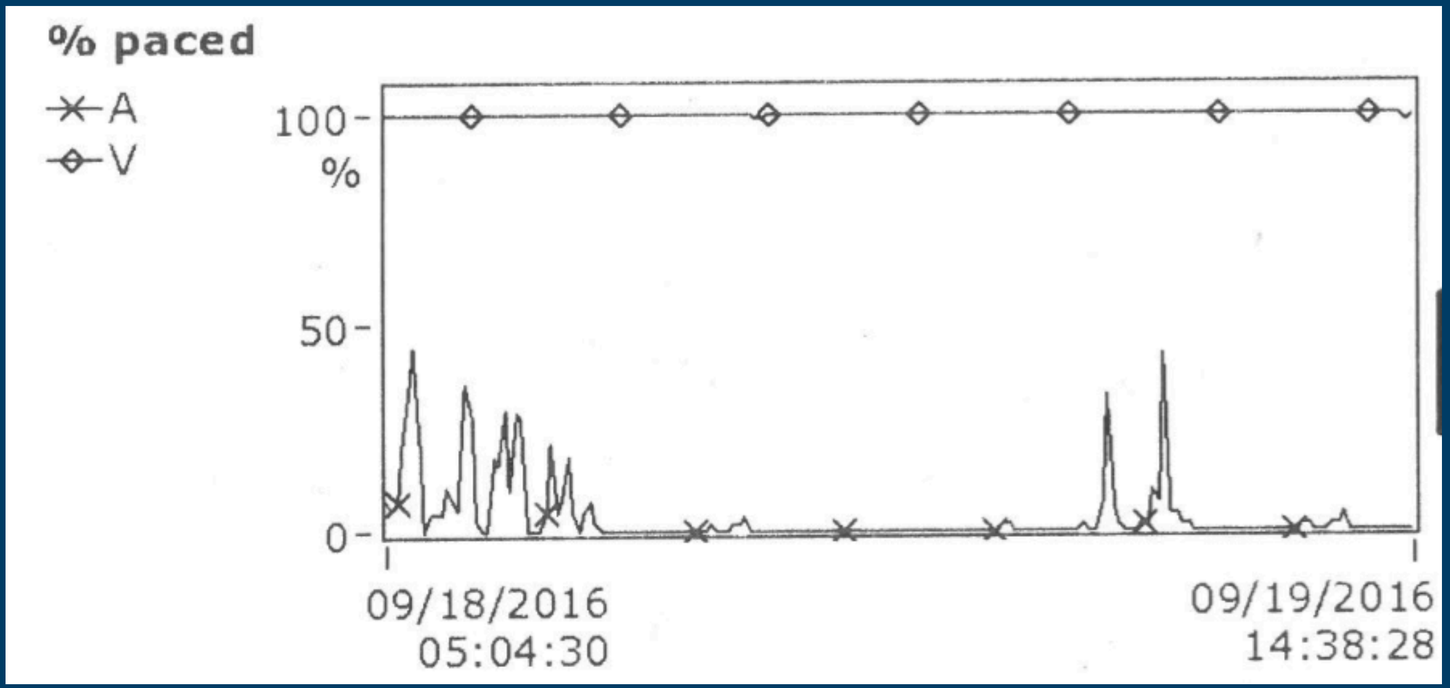
CYBERSIKKERHET I MIN PERSONLIGE KRITISKE INFRASTRUKTUR

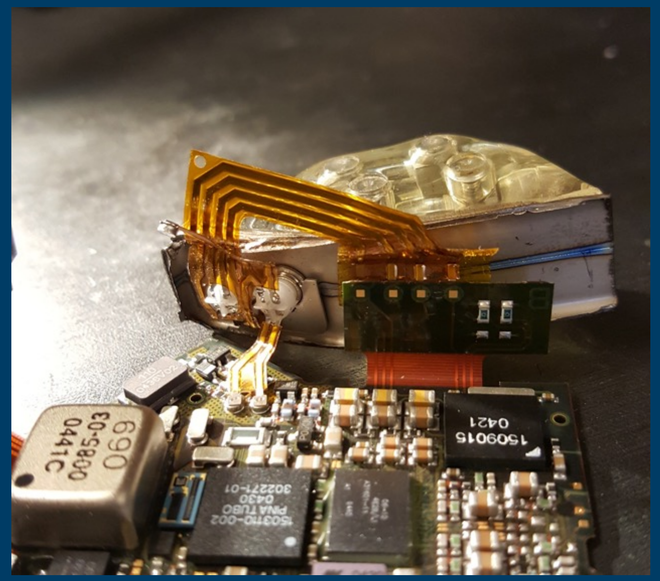
Marie Moe, SINTEF Digital

@MarieGMoe @SINTEF_Infosec

MIN PERSONLIGE KRITISKE INFRASTRUKTUR







SINTEF

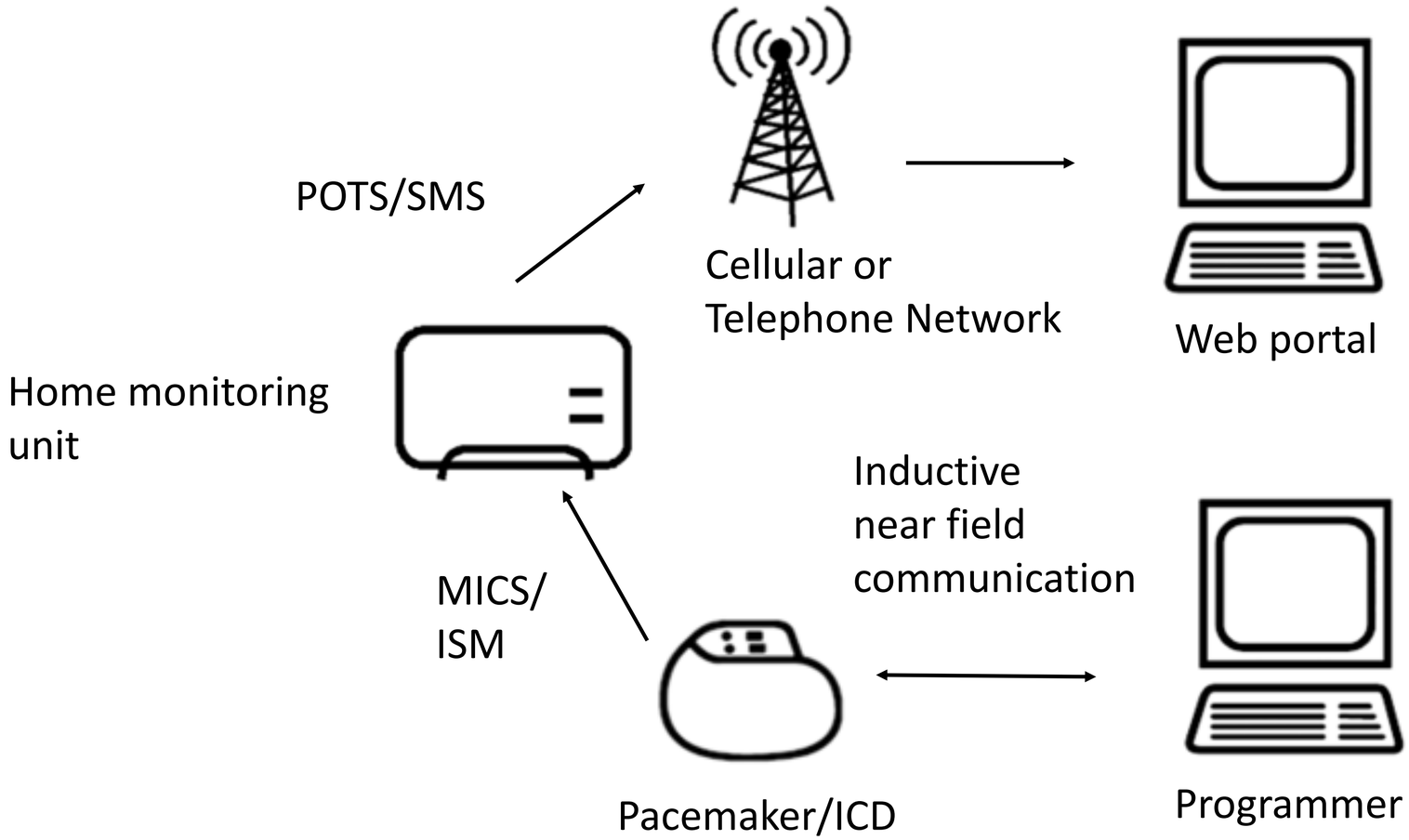
HVORFOR STARTE ET HACKING PROSJEKT?

- Proprietære løsninger
- Mangel på åpenhet fra leverandør
- Utdatert teknologi + tilkobling til internett = større angrepsflate

UTFORDRINGER FOR SIKKERHET I MEDISINSK UTSTYR

- Leverandør krever hull i brannmur for fjerntilgang
- Standard eller hardkodede passord, dårlig nøkkelhåndtering
- Ikke implementert tilfredsstillende mekanismer eller rutiner for software-oppdatering
- Det fysiske produktet har lang levetid og blir hengende etter i forhold til nye sikkerhetsmekanismer og utviklingen i trusselbildet
- Produkter som tradisjonelt har fungert i lukkede miljø kobles på nett
- Mangelfull regulering og lovverk
- Lav bruker- og bestillerkompetanse

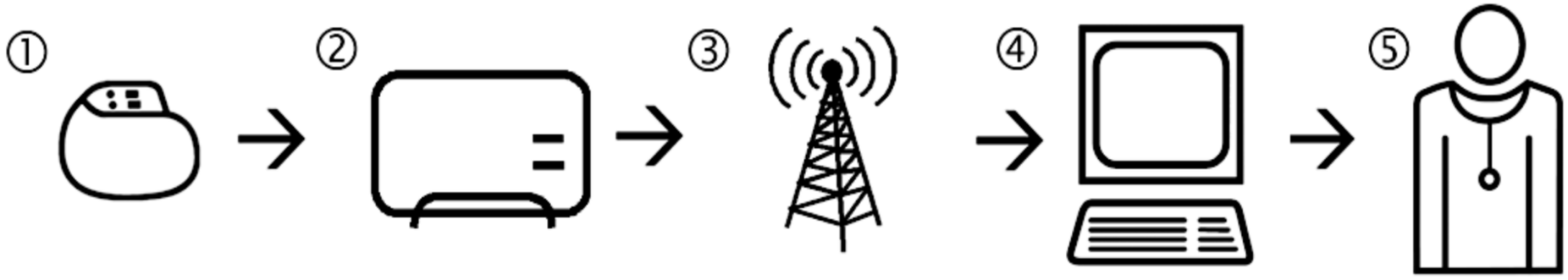
KOMMUNIKASJONSGRENSESNITT




Merlin@home
Transmitter
ST. JUDE MEDICAL
BIOTRONIK
OK 2
Medtronic
MEDTRONIC CARELINK® MONITOR

HVA KAN GÅ GALT?

- Sårbarheter i pacemakeren?
- Sårbarheter i aksesspunktet?
- Kan vi stole på mobilnettet?
- Er leverandørens servere/skytjeneste sikret?
- Sårbarheter i webportalen? Menneskelige feil?



St. Jude Medical, Inc.
NYSE: STJ - 30. aug., 05.27 EDT

78,25 USD ↑0,24 (0,31 %)
Før åpningstid: 78,70 ↑0,58 %

1 dag | 5 dager | 1 måned | 3 måneder | 1 år | 5 år | Maks.

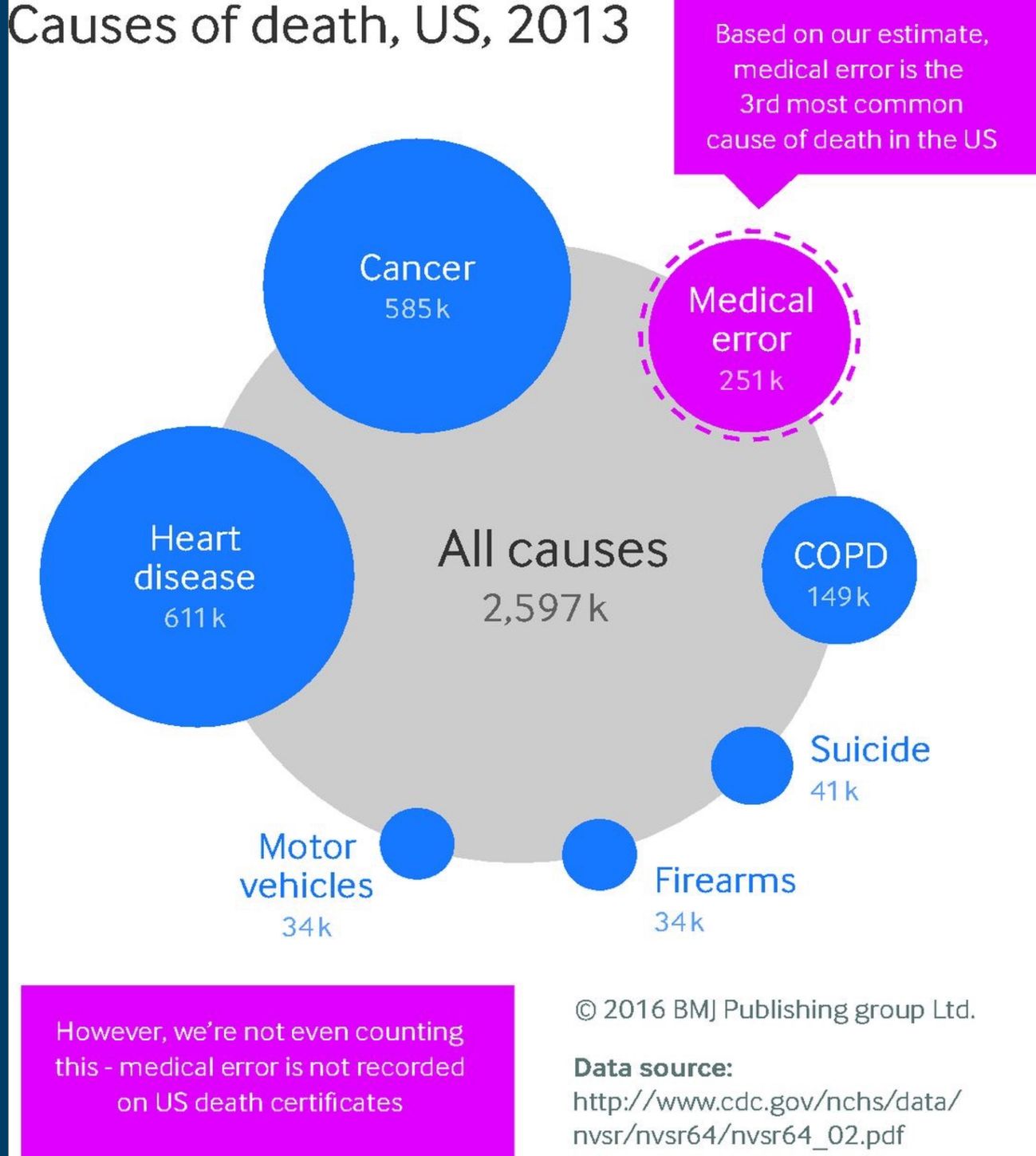
84
82
80
78
76
74
24. aug.
25. aug.
26. aug.
29. aug.

St. Jude stock shorted on heart device hacking fears; shares drop

The stock of pacemaker manufacturer St. Jude Medical Inc (STJ.N) fell sharply on Thursday after short-selling firm Muddy Waters said it had pl...

MEDISINSK UTSTYR BÅDE REDDER LIV OG TAR LIV

- Mangel på rapportering av uønskede hendelser
- Manglende testing av bruker-vennlighet og sikkerhet
- Manglende logging og etterforskning av hendelser



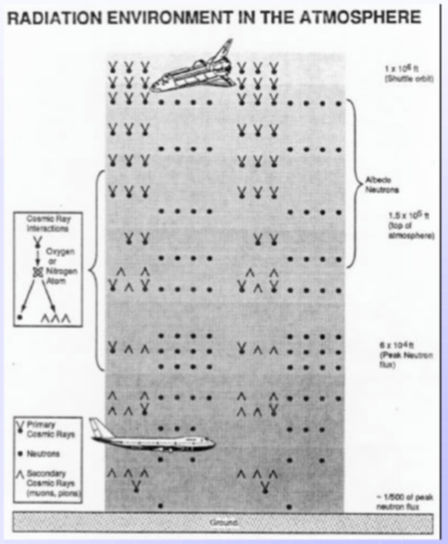
KOSMISK STRÅLING GA MEG TILGANG TIL KODEN

BOEING PHANTOM WORKS

Neutron Environment in the Atmosphere

Boeing Radiation Effects Lab

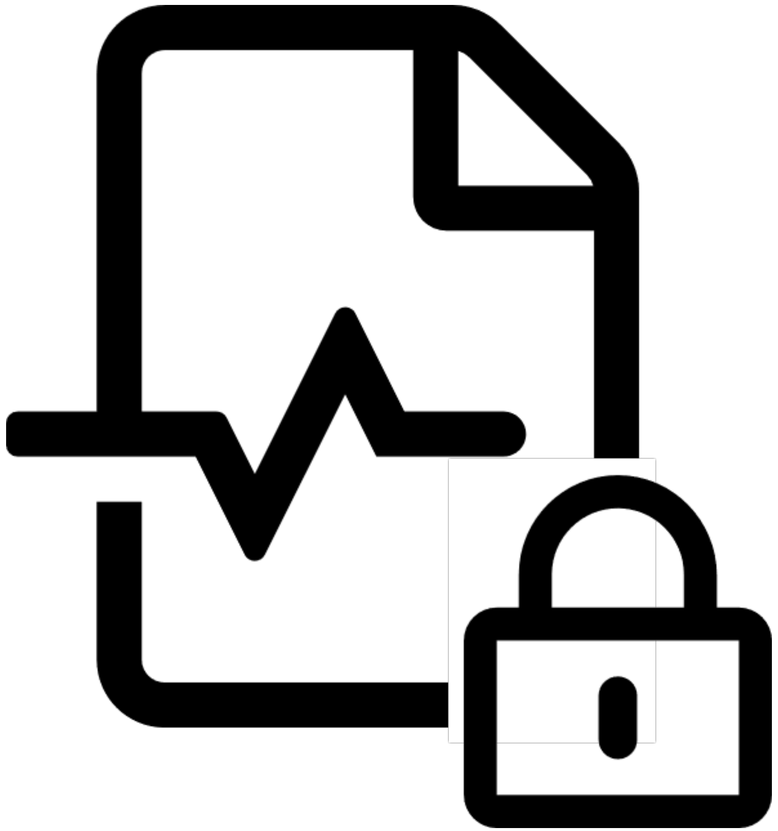
Neutrons, created by cosmic ray interactions with the O_2 and N_2 in the air, peak at ~60,000 ft. At 30,000 ft the neutrons are about 1/3 the peak flux, and on the ground, ~1/400 of the peak flux. The peak flux is ~4 neutron/cm²sec. Other particles such as secondary protons and pions are also created, but for SEU the neutrons are the most important.

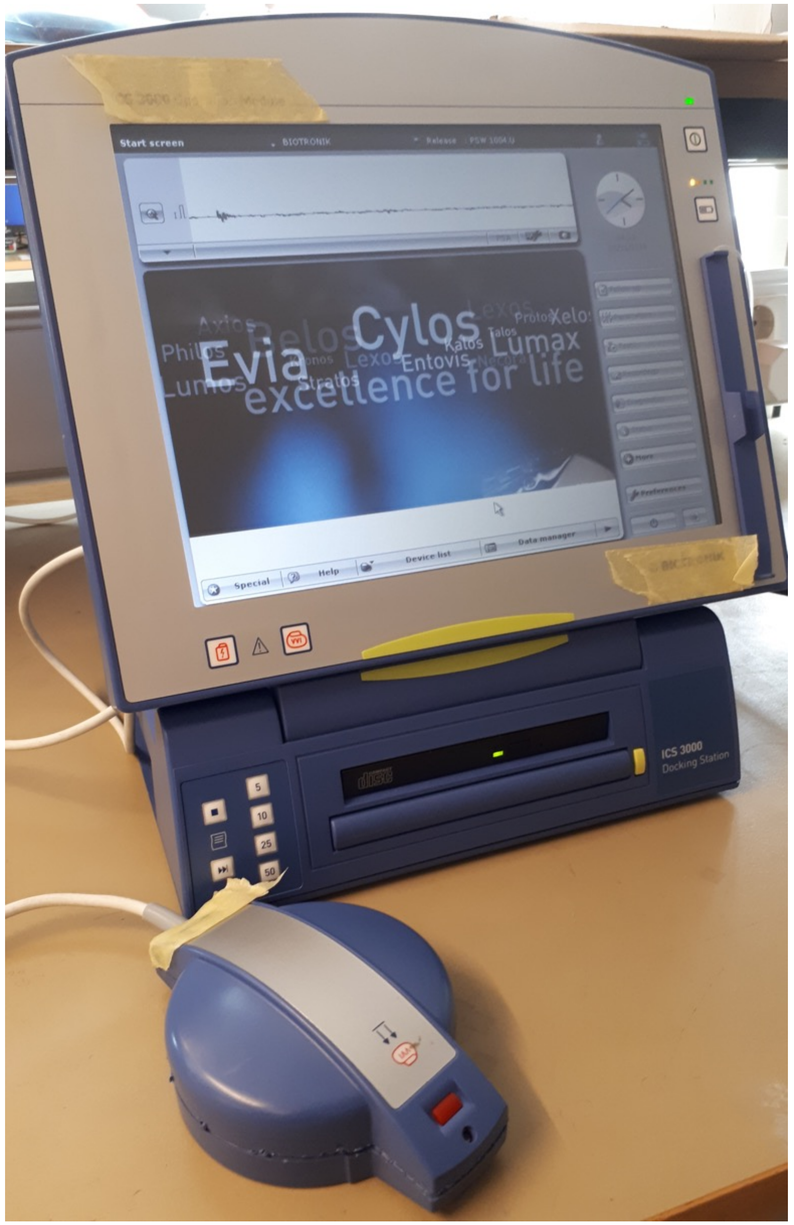


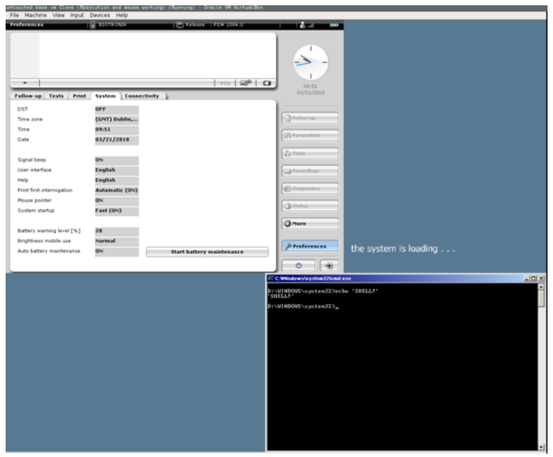
1/4/99

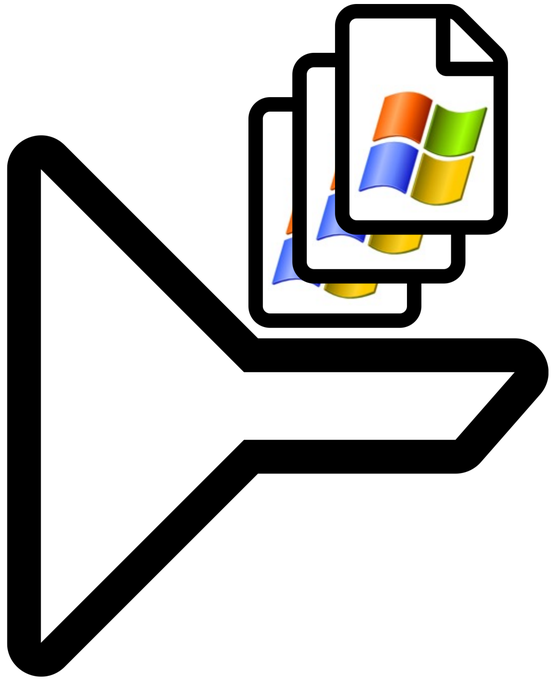
5

EN KRYPTERT ZIP-FIL MED MIN PASIENTDATA









Microsoft Internet Explorer 6

Acrobat® Reader™ 5.0
There's more to Acrobat than Reader!

Kithara

Chilkat Software
inventing power with simplicity

BIOTRONIK

RENESAS
Everywhere you imagine.

```
    loc_463BC267:
0A0 mov     edx, offset a9biotronikzip7 ; "9BiotronikZI
0A0 mov     eax, [ebp+Zip2Obj]
0A0 call    ck_unlock
0A0 mov     ecx, 3          ; encryption_mode_type
0A0 mov     edx, 21h        ; encryption_property
0A0 mov     eax, [ebp+Zip2Obj] ; this
0A0 call    set_property
0A0 mov     ecx, 100h       ; keysize
0A0 mov     edx, 22h        ; keysize_property
0A0 mov     eax, [ebp+Zip2Obj] ; this
0A0 call    set_property
0A0 mov     edx, offset aBiotronik ; "BIOTRONIK"
0A0 mov     eax, [ebp+Zip2Obj]
0A0 call    setpw_or_encpw
0A0 lea     eax, [ebp+var_4C]
0A0 mov     edx, [ebp+var_8]
0A0 call    @System@@WStrFromLStr$qqrr17System@WideStri
0A0 mov     edx, [ebp+var_4C]
0A0 mov     eax, [ebp+Zip2Obj]
0A0 call    sub_463BB960
0A0 mov     eax, [ebp+var_4]
0A0 cmp     dword ptr [eax+4], 0
0A0 jnz     short loc_463BC2D6
```

```
Chilkat.Zip zip = new Chilkat.zip();
zip.UnlockComponent("License String");
zip.Encryption = 3;
zip.EncryptionKeyLength = 256;
zip.EncryptPassword = "Password"
```

HVORDAN FÅ BEDRE SIKKERHET?

- **Cybersafety-by-design**: Sikkerhet i programvareutviklingsløpet for medisinsk utstyr hos produsenter og i hele leverandørkjeden
- **Bevissikring:** Bevissikring og logging vil kunne brukes i hendelseshåndtering og etterforskning i etterkant av en hendelse der medisinske implantat kan ha blitt utsatt for cyberangrep
- **Testing**: Metodikk og rammeverk for tredjeparts testing
- **Patching:** Løsninger for rask og sikker patching av sårbarheter og sikkerhetshull i medisinske implantat
- **Resilience:** Hvordan sørge for at komponenter i det medisinske implantatet fortsetter å levere kritisk pasientbehandling også under feiltilstander eller forsøk på angrep

KONKLUSJON

Vår avhengighet av systemer som styres av programvare øker raskere enn vår evne til å sikre systemene

- Utstyrsprodusenter må bygge inn sikkerhet i produktene
- Brukere må gjøre egne risikoanalyser og følge med på utviklingen i risikobildet
- Vi må innse at det vil gå galt, og planlegge for dette
- Mer uavhengig forskning og tredjeparts testing trengs
- Standardisering, ansvarsavklaring og bedre lovregulering

Takk!

marie.moe @ sintef.no

www.infosec.sintef.no

@MarieGMoe @SINTEF_Infosec

SINTEF

RELATERT FORSKNING

Pacemakere:

- Dr. Kevin Fu et al (University of Michigan):
  - Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses (2008)
- Eduard Marin et al (KU Leuven):
  - On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them (2016)
- Barnaby Jack
- MedSec/Muddy Waters

Annet medisinsk utstyr:

- Hardkodede passord og “medical device honeypots” (Scott Erven)
- Medisinpumper (Billy Rios, Jeremy Richards)
- Insulinpumper (Jay Radcliffe)
- Farlige brukergrensesnitt (Harold Thimbleby)

SINTEF