Privacy is the cornerstone of personal safety

Karin Spaink

BobCatsss 2012

Trading privacy for security

Increased data collection, aka ‘counterterrorism’

- Tracking communication
- Tracking money
- Tracking people
- Tracking goods

BIG BROTHER

IS WATCHING YOU

Washington Post, July 2010

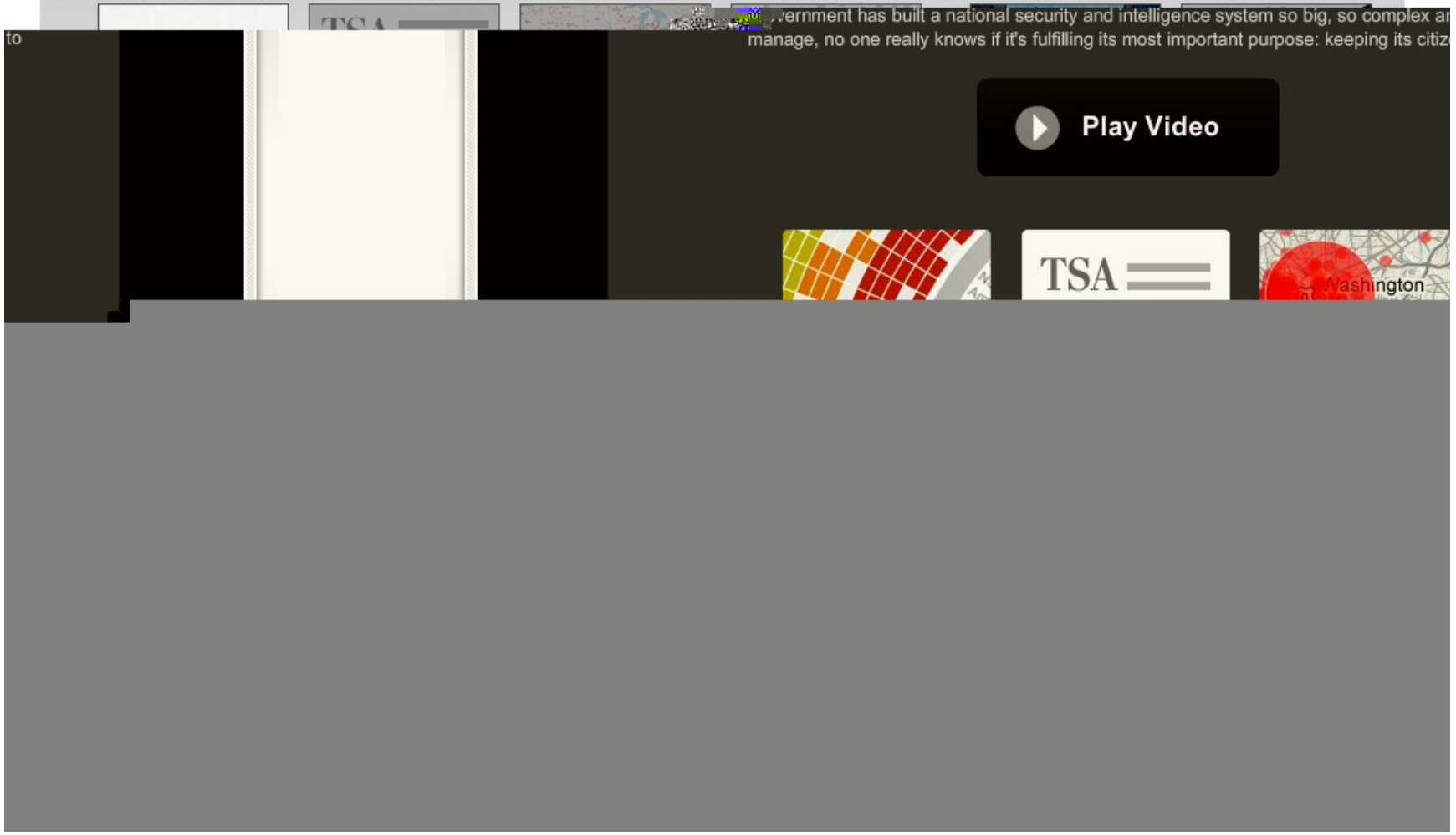
- Published *Top Secret America*
- After two years of research & FOIA's
- Investigation of counterterrorism agencies and their work
- Excluding 'common' surveillance

TOP SECRET AMERICA

A Washington Post Investigation

SHARE TSA

WATCH THE INTRO | READ THE STORIES | SEE THE MAP | EXPLORE CONNECTIONS | FIND COMPANIES | SEARCH THE DATA



Washington Post, July 2010

- 1271 government agencies (+263 since 9/11)
- 1931 external companies hired
- 10,000 high tech secured buildings
- 845,000 people with high security clearance
- $1.3 billion in 2003 → $31 billion 2010

Washington Post, July 2010

Increasingly minute investigations:

- NSA is sifting through 1,7 billion emails and phone conversations *per day*
- TSA is scrutinizing every passenger, both before flight and during check-in
- etc

Washington Post, July 2010

Results:

- Everybody is mostly *reprocessing* information
- Every report is becoming 'highly classified'
- Agencies don't co-operate / share. They *hide*
- Intelligence structure has become obtuse
- Expertise is wearing thin

‘Top Secret America’

- Missing reported information
  - Major Nalik Hassan, who shot 13 people and wounded 30 in November 2009 in Fort Hood, Tx
  - Umar Farouk Abdulmutallab, who planned a 2009 Xmas attack on a flight from Jemen to Detroit
- Too many people with high sec clearance
  - Bradley Manning

‘Top Secret America’

Eroding civil rights:

- Snooping is becoming the standard
- Assumption of innocence has become assumption of suspicion
- Body scans, now even in streets
- General idiocy (TSA cupcakes)
- Agencies go unchecked

(take a breath)

Can you maintain that this data collecting is:

- Efficient (doing its job)
- Proportional (minimizing intrusion)
- Not harmful or damaging
- Has increased your safety?

Other data

Everybody is collecting data:

- Facebook, Google (yeah)
- Public conveyance
- Camera's in streets and shops
- Memberships, loyalty programs
- Even cinema's, restaurants etc.

Other data

- ‘We can provide better service’
- …because they can demand it
- Amounts to trading privacy
- Sometimes for a bonus

Other data

- Everybody stores everything
- Data storage is dirt cheap
- Unclear what is done with data
- Often processed elsewhere
- (by companies that you do *not* have an agreement with)

Data breaches

- Not securely stored
- Not properly protected
- No ‘awareness’ of its importance

7. June 06, 2010: City sends wrong file
8. May 28, 2010: Sensitive DoJ data published
9. May 19, 2010: 75% of NL companies have leaked data
10. May 18, 2010: Travelers' info leaked
11. May 04, 2010: Bank dupes duped
12. Mar 01, 2010: Data of medical applicants leaked
13. Feb 27, 2010: Tax papers of civil servants leaked
14. Feb 26, 2010: Data of candidates 2006 election leaked
15. Feb 25, 2010: Student info often leaked
16. Feb 25, 2010: Data of hundreds of politicians leaked
17. Feb 08, 2010: Notary puts clients passports online
18. Feb 05, 2010: City Hall leaks e-mail addresses
19. Feb 05, 2010: Secret service leaks employee mail addresses
20. Jan 29, 2010: University of Utrecht leaks pay slips
21. Jan 27, 2010: Dpt of Public Works leaks subscribers' data
22. Dec 17, 2009: Bank employee loses USB stick
23. Nov 24, 2009: Social services leak e-mail addresses
24. Sep 08, 2009: Government leaks credit card numbers
25. Aug 12, 2009: Press agency leaks contact database
26. June 23, 2009: Stayokay hotel bookings leaked
27. June 17, 2009: Emergency info leaked online
28. May 30, 2009: Two telco's hand over sms contents to intelligence service
29. May 08, 2009: Hoster Vuurwerk/Tele2 leaks e-mail addresses
30. May 04, 2009: Newspaper leaks e-mail addresses
31. Apr 29, 2009: City police leaks e-mail addresses
32. Apr 06, 2009: Dispute Committee website reveals all
33. Mar 31, 2009: Magazine leaks new subscribers
34. Mar 30, 2009: Bike locker codes up for grabs
35. Mar 24, 2009: Police site leaks speeding pictures
36. Feb 10, 2009: Free condom site leaks customer data

Afbeelding 'Old log book' van Admond onder Attribution 2.0 Generic licentie

Datalek: Gemeente Meppel lekt ID-kaarten

19 jan / 03:41 pm
Door Oliver Bruno

categorie: Zwartboek Datalekken

Bits of Freedom heeft haar Zwartboek Datalekken alweer uitgebreid. De website van de gemeente Meppel lekt kopieën van identiteitskaarten, burgerservicenummers en mailtjes met ambtenaren.

Via de gemeentelijke website zijn 1.700 dossiers van vergunningaanvragers met hierin burgerservicenummers, handtekeningen en zelfs kopieën van identiteitskaarten van burgers te downloaden. Verder waren handgeschreven notities en e-mails van inwoners aan ambtenaren publiekelijk toegankelijk. Het lek werd aan het licht gebracht door een 26-jarige internetgebruiker. De documenten en gegevens waren toegankelijk door de bovenliggende directories te benaderen van een webadres. Dat kan door het met de hand aanpassen van het adres in de adresbalk van de browser. De technische term hiervoor is *directory traversal*. Google had de bestanden ook al gevonden en de documenten waren binnen zes

LEES MEER

16 JAN 2012 Datalek: Beauty.nl en Recreatief.nl lekken 315.000 gegevens
Oliver Bruno — 0

8 JAN 2012 Datalek: Udense vuurwerkhandel lekt klantenbestand
Oliver Bruno — 0

22 DEC 2011 Wetsvoorstel meldplicht datalekken. Eindelijk!
Rejo Zenger — 3

15 DEC 2011 Datalek: KPN lekt klantgegevens Gemnet
Oliver Bruno — 0

Data safety

- How to properly store, process, access data
- Breaches have unexpected consequences
  - Jeremy Clarke, Top Gear
  - ID theft
  - Mobile bought with stolen ID
  - Loans, mortgages
- If a company wants it, *they* say it's important

Semmelweiss

- Introduced the notion of hygiene
- Has become widely accepted
- Plastic wrappings, sterilized material, clean water, wash & shower, don't drink from puddles or eat from floor
- Backed up by laws, procedures and education

Data hygiene

- No USB sticks, CDs and DVDs
- No laptops in company LAN
- Database compartmentalization
- Encryption
- Password protection plans

- Sloppiness needs to become ‘dirty’

Data hygiene

Concept needs to be implemented by:

- Publication of best practices
- Rules and regulations
- Obligation to notify
- Fines

Executive summary

Recent high profile incidents of personal data loss across Europe have prompted wide discussion on the level of security given to personal information shared, processed, stored and transmitted electronically. Gaining and maintaining the trust and buy-in of citizens that their data is secure and protected represents a potential risk to the future development and take up of innovative technologies and higher value added online services across Europe and will be a key challenge for organisations going forward.

The introduction of a European data breach notification requirement for the electronic communication sector introduced in the review of the ePrivacy Directive (2002/58/EC[1]) is an important development with a potential to increase the level of data security in Europe and foster reassurance amongst citizens on how their personal data is being secured and protected by electronic communication sector operators. Against this background, ENISA aims to review the current situation and to develop a consistent set of guidelines addressing the technical implementation measures and the procedures, as described by Article 4 of the reviewed Directive 2002/58/EC.

The telecommunications sector recognises that data breach notifications have an important role in the overall framework of data protection and privacy. Nevertheless, operators are seeking support and guidance on an EU and local level over a number of issues, which if clarified, would better enable European service providers to comply effectively with data breach notification requirements. Key concerns raised by telecom operators include the following:

- **Risk prioritisation** – The seriousness of a breach should determine the level of response. In order to prevent 'notification fatigue' for both the operator and the data subjects, breaches should be categorised according to specific risk levels

- **Communication channels** – Operators want assurances that notification requirements will not negatively impact their brands. It is important for operators to maintain control of communications with relevant data subjects, as much as possible, to ensure that operators can effectively manage any impact on brand perception brought about

EU proposal

- Mandatory notification of data breaches
- Must be quick and informative
- Public exposure of worst offenders
- Issuing awards for exemplary behavior
- Fines, up to 5% of gross global turnover

Additionally

- Makes data handling more expensive
- Might stop unwarranted collection of data
- Perhaps implement bounty for data breach hunters?

But:

We should start thinking about protecting *machines*, too:

- Cars (opening doors, alcohol locks)
- Houses (domotic appliances)

Medical data

Electronic patient records

- Patient files lost, stolen or sold
- Many hospitals have had computer viruses
  - Mytob virus (2005), 3 UK hospitals in *2008*
- Hack in 2005: 1.2 million patient records

```
"polisnummer","vrl","naam","telefoonnummer","geboortedatum","polis
nummer","adres","huisnummer","postcode","woonplaats"


99xxxxxxx,B.,Waxxxxxxxx,05xxxxxxxx,Jul  7 2004
 12:00AM,99xxxxxxx,xxxxxxxxstr,11,xxxx TC,xxxxxxx
01xxxxxxxx,E.J.,Kaxx,07xxxxxxxx,Jan  2 1962
 12:00AM,01xxxxxxxx,xxxxxxxxxxxln,30,xxxx ND,xxxxxxxxx
34xxxxxxx,R.,Bexx,03xxxxxxxx,Jul  7 2004
 12:00AM,34xxxxxxx,xxxxxxxdiep,19,xxxx NR,xxxxxx
00xxxxxxx,F.M.,Vexxxxxx,06xxxxxxxx,Jul 13 1979
 12:00AM,00xxxxxxx,xxxxxxxxln,46,xxxx VA,xxxxxx
06xxxxx,N.C.,Boxx,07xxxxxxxx,May 18 1994
 12:00AM,06xxxxx,xxxxxxxxxstr,3,xxxx BH,xxxxxx
77xxxxxxx,L.,Lexxx,05xxxxxxxx,Jul  7 2004
 12:00AM,77xxxxxxx,xxxxxxxxxstr,17,xxxx XP,xxxxxx
77xxxxxxx,L.H.,Scxxxxxx,03xxxxxxxx,Jul  7 2004
 12:00AM,77xxxxxxx,xxxxxxxxxsluis,34,xxxx EB,xxxxxxxxx
77xxxxxxx,B.,Maxxxxx,06xxxxxxxx,Jul  8 2004
 12:00AM,77xxxxxxx,xxxxklauw,19,xxxx GV,xxxxxx
95xxxxxxx,N.,Baxxxxx,05xxxxxxxx,Apr 21 1993
 12:00AM,95xxxxxxx,xxxxtuin,51,xxxx ZX,xxx
20xxxxxxx,A.M.,Ogxxxxx,03xxxxxxxx,May  8 1972
 12:00AM,20xxxxxxx,xxxxxxxxxxxxwg,29,xxxx BT,xxxxxx
81xxxxxxx,D.,Boxx,03xxxxxxxx,Jul  8 2004
 12:00AM,81xxxxxxx,xxxxxxxxxxwg,23,xxxx HC,xxxxxx
92xxxxxxxx,E.,Rexxxxxx,03xxxxxxxx,Jul  8 2004
 12:00AM,92xxxxxxxx,xxxxxxstr,16,xxxx VL,xxxxxx
40xxxxxxx,G.G.,Boxxx,03xxxxxxxx,Oct  8 1955
 12:00AM,40xxxxxxx,xxxxxxde,10,xxxx HD,xxxxxxxxx
```

"PatientCode","BesmettingTypeID","IngelichtDoor","Opmerking"

10xxx,4,beh.arts,Patient bekend met MRSA inmidd,
10xxx,2,behandelnd arts,ESBL positief. bij opname: con,
25xxx,4,arts,Tot 05-01-2003 MRSA verdacht. ,
28xxx,4,niet,Mogelijk contact met MRSA B6 W,
38xxx,4,arts,Tot 05-01-2002 MRSA verdacht. ,
43xxx,4,verpleeghuisarts,Patient is MRSA positief. Bij ,
46xxx,4,behandelend arts,patient bekend met MRSA. MRSA ,
51xxx,4,huisarts,Strikte isolatie volgens MRSA ,
51xxx,4,niet,Mogelijk contact met MRSA B6 W,
55xxx,4,nog niet,Bij opname in strikte isolatie,
69xxx,4,behandelend arts,tot 01-07-2003 verdacht van MR,
75xxx,4,Dr. Hxxxxx,Dhr. is positief voor MRSA, Bi,
76xxx,2,behandelend arts,Bij opname in contactisolatie.,
81xxx,4,arts,bij opname: isolatie op een ka,
81xxx,4,van den xxxx neurolo,Bij opname patient isoleren al,
85xxx,4,,MRSA verdacht tot 12-02-2003. ,
10xxxx,4,xxxxxx Blxxxxx,Dhr. is positief geweest. Bij ,
10xxxx,4,arts,bij opname: isolatie op kamer,
10xxxx,4,hygienist,Bij opname MRSA protocol, stri,
10xxxx,4,arts,Bij opname: isolatie op een ka,
11xxxx,4,behandeled arts,MRSA positief. Opname op een e,
13xxxx,4,verpleeghuisarts,Patient is bekend met MRSA
24xxxx,4,ziekenhuishygienist,MRSA positieve patient. Bij o,
26xxxx,4,hygienist,Contactisolatie,schort en hand,
26xxxx,2,arts,ESBL-positief, Enterobacter, b,
28xxxx,4,ziekenhuishygienist,Bij opname in strikte isolatie,
30xxxx,4,xxxxxx Abxxx,,

Medtronic

Pacemaker, wireless hack in May 2008:

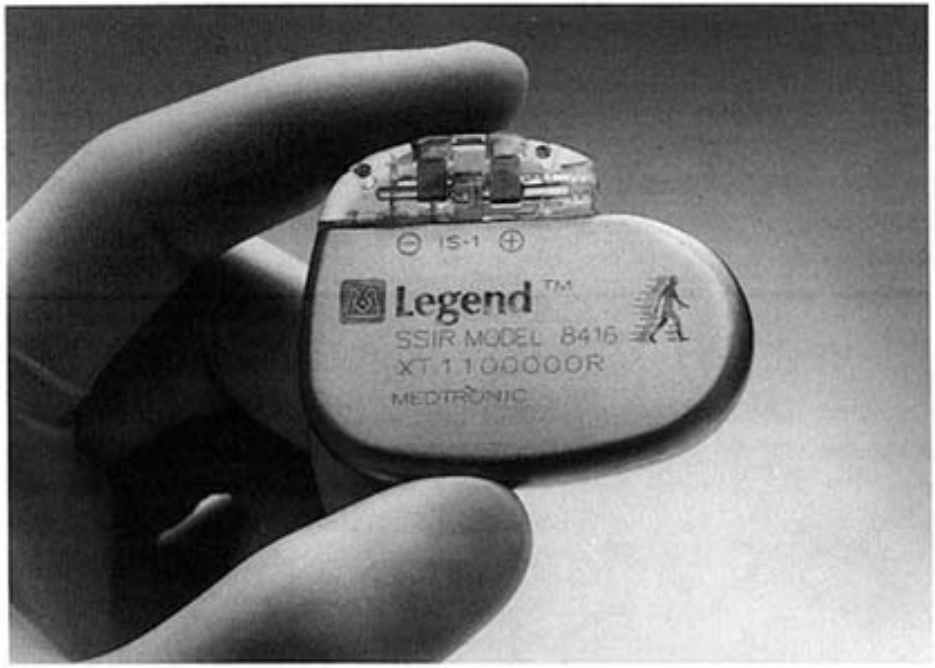
"…this has very serious implications for the 2.6 million people who had pacemakers installed from 1990 to 2002. It also presents product liability problems for the five companies that make pace makers."

http://venturebeat.com/2008/08/08/defcon-excuse-me-while-i-turn-off-your-pacemaker/

Defcon: Excuse me while I turn off your pacemaker

August 8, 2008 | Dean Takahashi

45 Comments



The Defcon conference is the wild and woolly version of Black Hat for the unwashed masses of hackers. It always has its share of unusual hacks. The oddest so far is a collaborative academic effort where medical device security researchers have figured out how to turn off someone's pacemaker via remote control. They previously disclosed the paper at a conference in May. But the larger point of the vulnerability of all wirelessly-controlled medical devices remains a hot topic here at the show in Las Vegas.

Medtronic

Response:

- It’s too expensive to execute this hack
- We don’t think it’s important enough

Medtronic

Insulin pump, wireless hack in August 2011:

- Some company, same hack
- Wireless, from a 500 m distance
- … and dirt cheap.
- Affected: 2 million people in the US

Maker of hacked insulin pump ignores risk and history of pacemakers with the same problem

Medtronic Maximo pacemakers were found in 2008 to be easily hacked and taken over

By **Kevin Fogarty** Add a new comment Like 1 +1 1

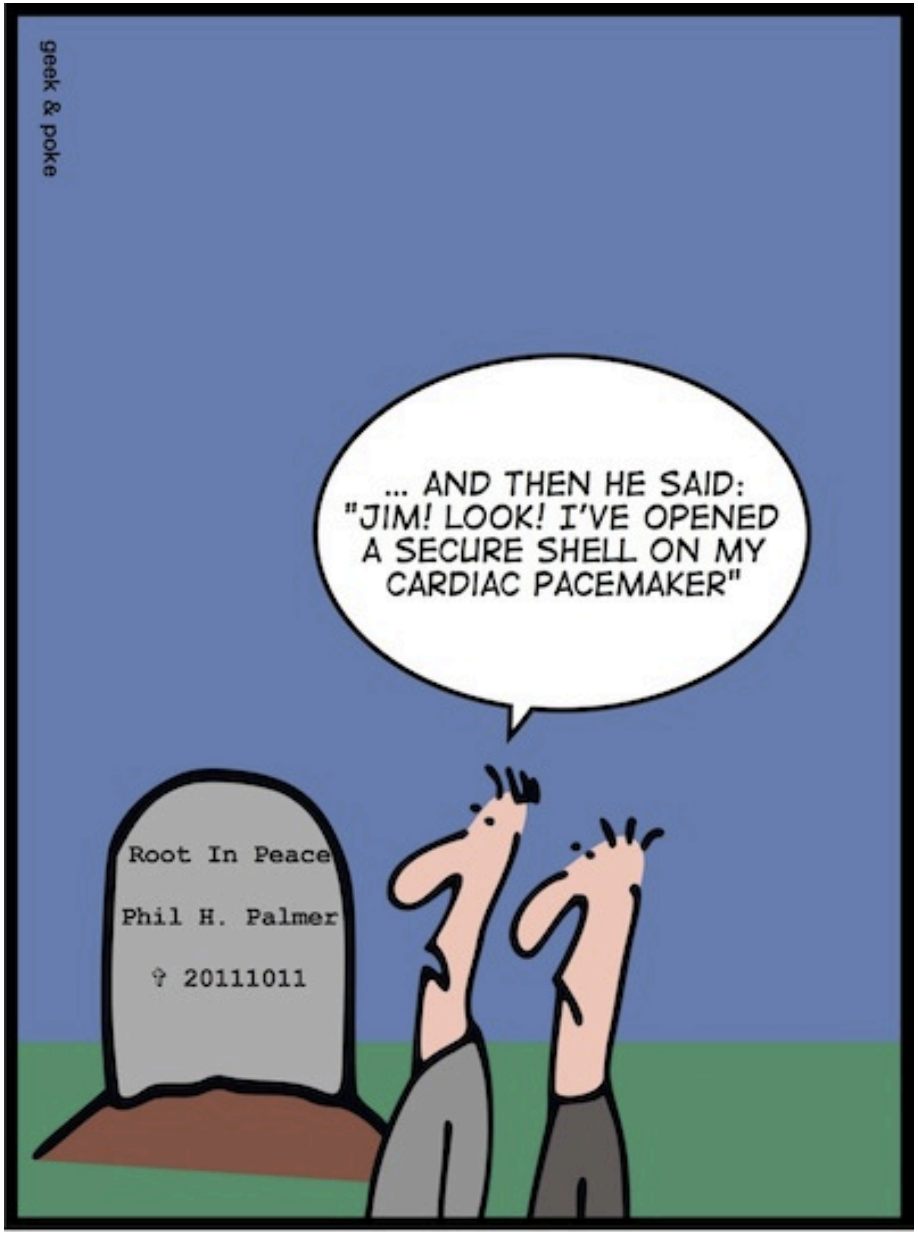
August 26, 2011, 2:33 PM — The most unexpected and inherently creepy hacking demonstration at this year's Black Hat conference was one from IBM security researcher Jay Radcliffe, who demonstrated how he was able to hack the wireless data connection on his insulin pump to take over and control it from as far as half a mile away.

He was able to increase or decrease his own dose to levels that would have been fatal, without any significant resistance from the pump, which lacked even the ability to identify whether commands were coming from a legitimate source.

Radcliffe didn't name the manufacturer in his Aug. 4 talk. He changed that during a press conference he called yesterday out of, he said, frustration at being stonewalled or ignored in three weeks worth of attempts to get Medtronic to talk about the huge security flaw and even huger potential legal liability Radcliffe found in its insulin pumps.

Medtronic

- ‘Uhm, we’ll try to fix it in later models…’
- Refused to speak with the hacker (Jay Radcliff, IBM)
- Meanwhile, their PR dept. got *very* active
- Should have had their FDA approval pulled


geek & poke
... AND THEN HE SAID: "JIM! LOOK! I'VE OPENED A SECURE SHELL ON MY CARDIAC PACEMAKER"
Root In Peace
Phil H. Palmer
† 20111011

Thank you

Your safety depends on your privacy,
not the other way around

karin@spaink.net
www.spaink.net