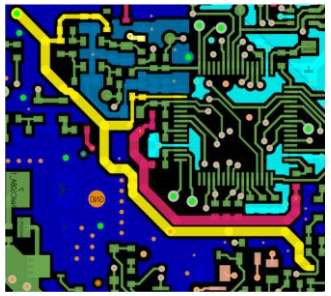
Why we fail at security…

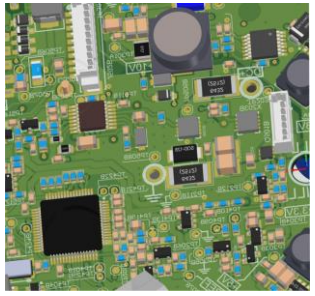
by Stefaan De Roeck

ELECTRONICS & APPLICATIONS
14 T/M 16 MEI 2019 JAARBEURS UTRECHT

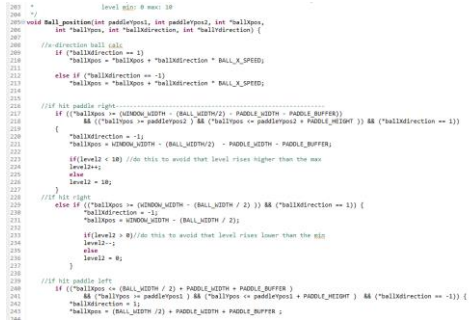
Electronic Development

PCB Layout 2D/3D and mechanical integration



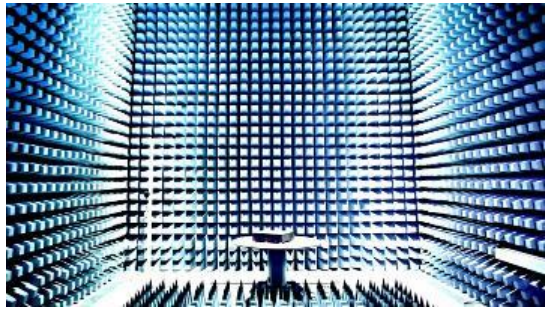


Firmware/Software

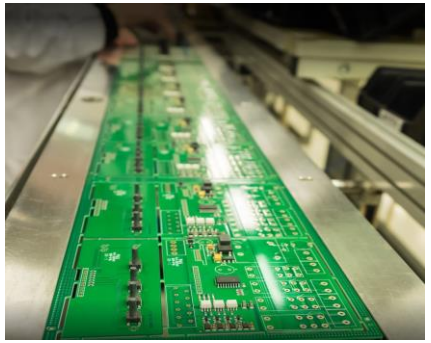


Prototypes

EMC / Testlab CE



Volume Manufacturing



Mechanical Engineering and Production

On site Consultancy

dekiMMo experts

Why we fail at security…

… much too often.

Contents

1. Illustration: Yes, we fail at security…
2. How did we get here?
3. Adding security, two real life stories
4. Root causes of products with bad security
5. Solutions

Illustration:
Yes, we fail at security

Security failure examples…

- Zigbee War Flying - Philips Hue
- Directory of on-line surveillance cameras – insecam.org
- Heartbleed
- Belgacom Hack
- Angela Merkel's Phone
- Huawei Controversy
- More
- …

Yes, we fail at security…

- Often
- With real impact on:
  - Functionality
  - Privacy
  - Broader security
  - Safety

Hacker’s intentions

- Hacks can be divided into mainly two categories:
  - Opportunistic
    1. Requirements:
       - A vulnerability (just published, just discovered, 0-day, …)
       - A strategy (goal + plan to make it happen)
    2. Scan a range of targets for susceptibility to the vulnerability
    3. Attack the target to obtain leverage
    4. Use leverage to contribute to goal
  - Targeted
    1. Requirements:
       - A specific target (usually comes with the goal)
       - Expertise in security, vulnerabilities, social engineering, …
    2. Scan / get to know the target, identify attack vectors, make a plan
    3. Execute
    4. Achieve the goal

How did we get here?

- A couple of things have happened:
  - Much more of our lives happens on-line:
    - 1) People's everyday lives
      - In case of outage, bigger impact – we notice it better
    - 2) Company staff
      - More dependence on IT systems
    - Hence also much more to be gained there:
      - Information
      - Access to bank accounts / funds…
  - Industry has jumped on the IoT bandwagon
  - We all have smartphones… and expect everything to connect easily
  - Things with value:
    - Visibility
    - Cryptocurrency
    - Information (-> targeted advertising, market research, …)
    - (Brand) reputation, politics, …

But we weren’t prepared…

- The IoT opportunity: existing product lines to which we want to add connectivity
- Yet, those companies:
  - Didn’t have the experience to add the connectivity features
  - (Understandably) have their primary interest focused on getting their products to the market first, and only later fix the problems…

Adding security to a product

A (anonymized) real-life story

Adding connectivity to a product: failure example

- Company designs and manufactures controllers for compressors
- Their products do not interface with customer's IP networks. However, for servicing, they support "field engineer access" to those devices over a dedicated network interface.
- So: adding the option to interface with remote controllers over IP, seems only a small technical increment…

Adding connectivity to a product: limitless opportunities

- Higher-end product – more options for the customer
- Attract new customers, those that require connectivity to begin with
- Easier monitoring, servicing, …
- Less need for physical presence
- Reduced cost
- …

But… then come the following questions

Adding connectivity to a product: what about security?

- Answer 1: We already have security. Our devices are designed to go into fail-safe when an alarm is triggered.
- Answer 2: Yes, security is indeed important. We don't want give our customer access to our IP.
- Answer 3: Ah, of course we don't want our product to be hacked. What should we do?

= helping to realize new challenges and extra design effort come with adding connectivity

Adding ~~connectivity~~ security to a product

- "Yes, we want to secure our products!"
- Against what?
  - IP theft (know-how, company secrets, counterfeiting, …)
  - Privilege escalation (too broad access for customer e.g.)
  - Third-party interference, impact on functionality (Denial-Of-Service, …)
  - Unauthorized third-party access

Adding security to a product

- All of these security concerns are different things
- Each attack vector warrants separate consideration, and usually results in separate countermeasures:
  - IP theft…
  - Unauthorized access by client…
  - DoS…
  - Unauthorized third-party access…

Adding security to a product: the “bargaining” phase

- “This is more than what I bargained for…”
- “Maybe our customers aren’t this determined to gain access…”
- “Maybe our customers aren’t sufficiently knowledgeable to gain access…”
- “Can’t we just do X, the result should be better than what we have now?”
- “Can’t we just ship it, and fix this later through a software update?”

- “We don’t have time now to do all this, we’ll have to continue this discussion later…

Adding security to a product: a probable end-scenario

- Technical current status: known and documented
- Development tracks towards implementing security goals: first steps documented
- Decisions wrt what kind of security steps: discussion dropped -> many things left undecided…
- Except: the perceived lowest-hanging fruit to do “something”
- The parting of ways & the mismatched perceptions:
  1. “This has been handled, they know what to do…”
  2. “So we’ll just… ignore the problem until it hits us in the face?”

Adding security to a workplace

Another (unfortunately) real-life story

One CEO talks to other CEO…

ELECTRONICS & APPLICATIONS
14 T/M 16 MEI 2019 JAARBEURS UTRECHT

But first some context:

- Small company / start-up
- Located in a business center
- Developing a (mainly) software application

"I would happily pay more in taxes, if somebody made me."

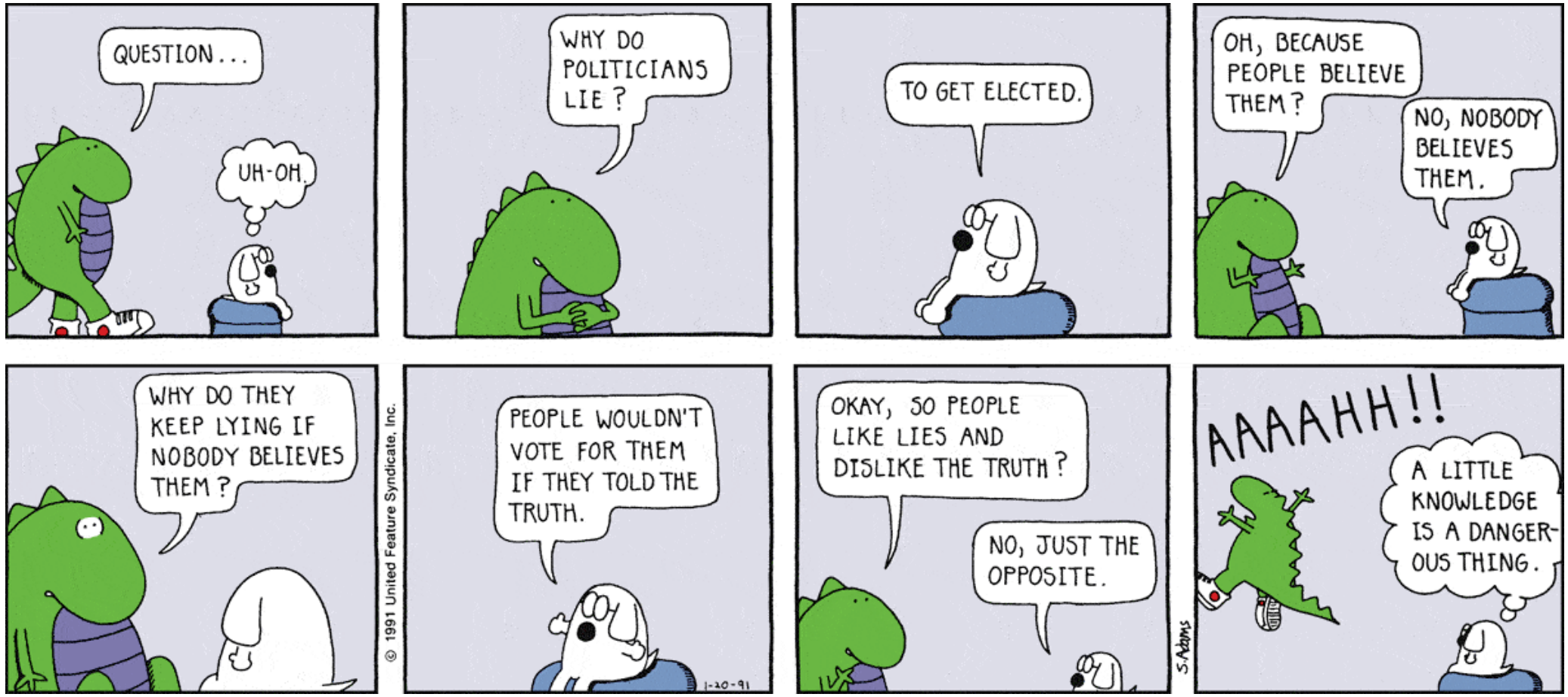
So the other CEO says:

- Did you know, recently, all WIFI networks' security is now broken?
- People can now just:
  - Park outside your building
  - Break into your network remotely
  - See everything you do
  - Steal your IP
  - And you'll never have seen them coming…
- I've banned all WIFI networking from my company, only wired is allowed.
- What about you?


A LITTLE KNOWLEDGE
can be
A DANGEROUS THING

- Reflexion:
  - There are >20 companies in a single office space
  - Superficial access control, which is worse than no control at all (false sense of security)
  - Lots of visitors
  - Open cubicles, easy access to wired Ethernet sockets, all on the same subnet
  - (Probably) a single Wi-Fi password for the whole floor
  - …

1. Wi-Fi protocol weaknesses are not your worst problem
2. You were already treating the Wi-Fi as an internet (>< intranet)



https://dilbert.com/strip/1991-01-20

Workplace security story, conclusion

ELECTRONICS & APPLICATIONS
14 T/M 16 MEI 2019 JAARBEURS UTRECHT

- Real security threat?
- Correct diagnosis?
- Appropriate remedy?
- How did it get this far?

Root causes for products with bad security

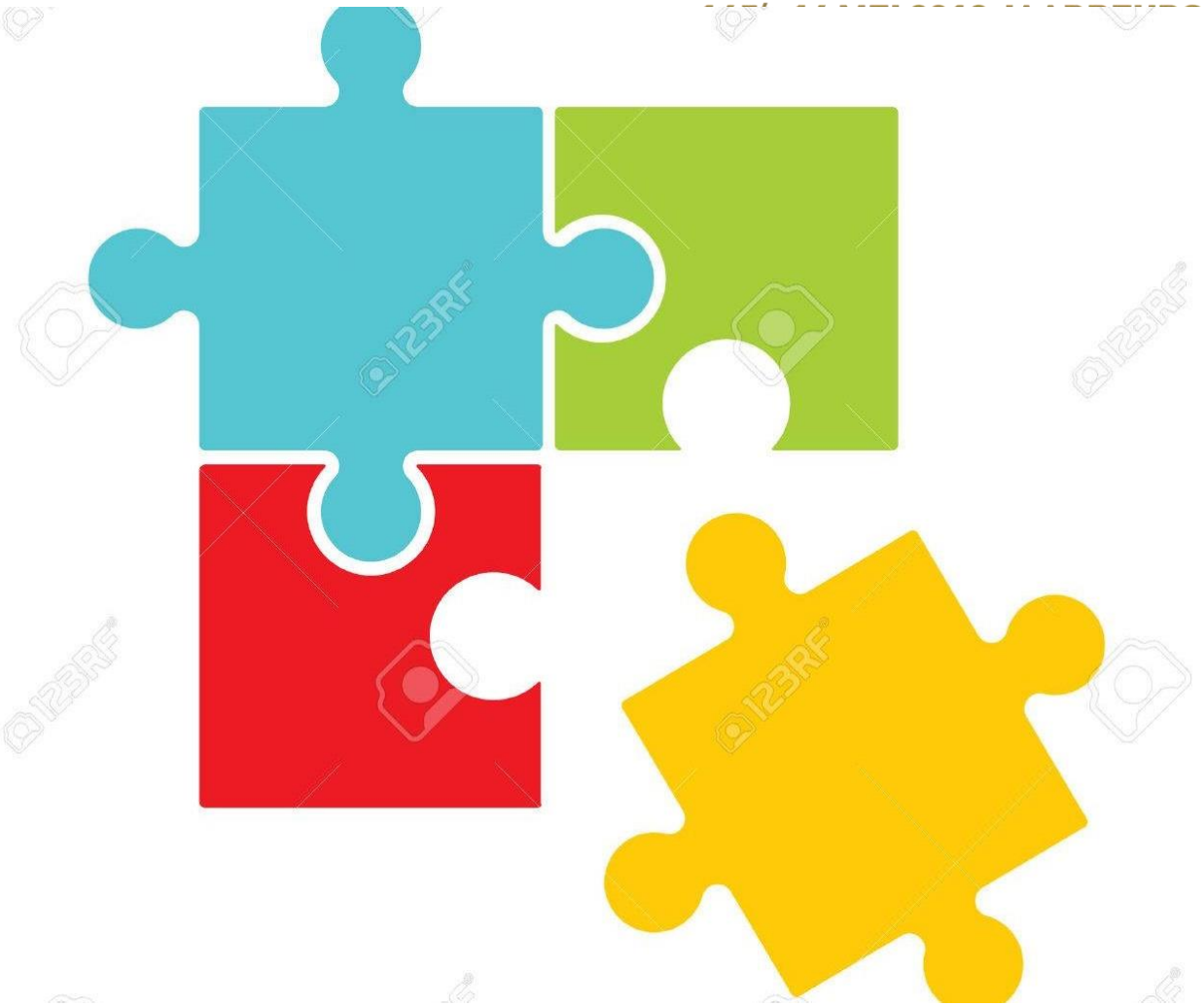
Security is a difficult topic

- Cyber security does not compare well to physical security
  - # possible break-in attempts / time
  - Likelihood that break-in goes unnoticed
  - Real-life guards get suspicious, cyber security systems much less so…
  - Authorization in cyber security is through challenge-response, not just be presenting a fixed token
- It’s based on difficult mathematics
- It’s still rather new (or: the audience has just increased in size)

Cause 1:
Understanding the technology (or lack thereof)

Security is NOT an add-on you can buy

Cause 2:
Existing products cannot easily be extended to “add security”



Technology changes fast, humans are set in their ways

Cause 3:
Maladjusted ways of designing, cooperating, support, maintenance, …

Problem summary

- “security” = overused word
- Security has:
  - become important quickly
  - for companies with (previously) unrelated core skills
  - that try to deal with it as they do with other product “features”
  - many aspects (theft, access, …)
- Time-to-market first, security later

- Digital security is hard to understand
- It’s not a pluggable add-on to a connected product
- Introducing connectivity and digital security in previously unconnected products = impact throughout whole company

People & companies don’t easily adapt

Solutions?

Legislation?

Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to institute a civil action to recover damages.

This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

This bill would become operative only if AB 1906 of the 2017–18 Regular Session is enacted and becomes effective.

Vote: majority Appropriation: no Fiscal Committee: yes Local Program: no

---

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.26. Security of Connected Devices

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

(1) Appropriate to the nature and function of the device.

Certification?

Conclusion

- Bring security into the core of your design work
- The technology is up for grabs
- Focus on:
  - Education
  - Awareness
  - Adapt processes

Thank you

ELECTRONICS & APPLICATIONS
14 T/M 16 MEI 2019 JAARBEURS UTRECHT

My contact details:

- Stefaan De Roeck
- stefaan.deroeck@dekimo.com

dekiMo experts

Your consultancy partner in high-tech (embedded) software and electronics engineering

Visit us in Hall 7, booth F024