# Usability for Privacy and Security

Jan Lühr, Senior Software Engineer & Architect
anderScore GmbH

TOPCONF Duesseldorf

anderScore trust in competence

# About me

**Jan Lühr**

Bachelor of Science, Computer Science

- Senior Software Engineer & Architect
- anderScore since 2007
- Focus
  - Pragmatic Architect
  - Build- and Deployment Engineering
  - Network- and Security-Techniques
  - RDMBS and NoSQL
  - IT-Trainer
- Java, JavaScript, Ruby

# Contents

1. Motivation 4

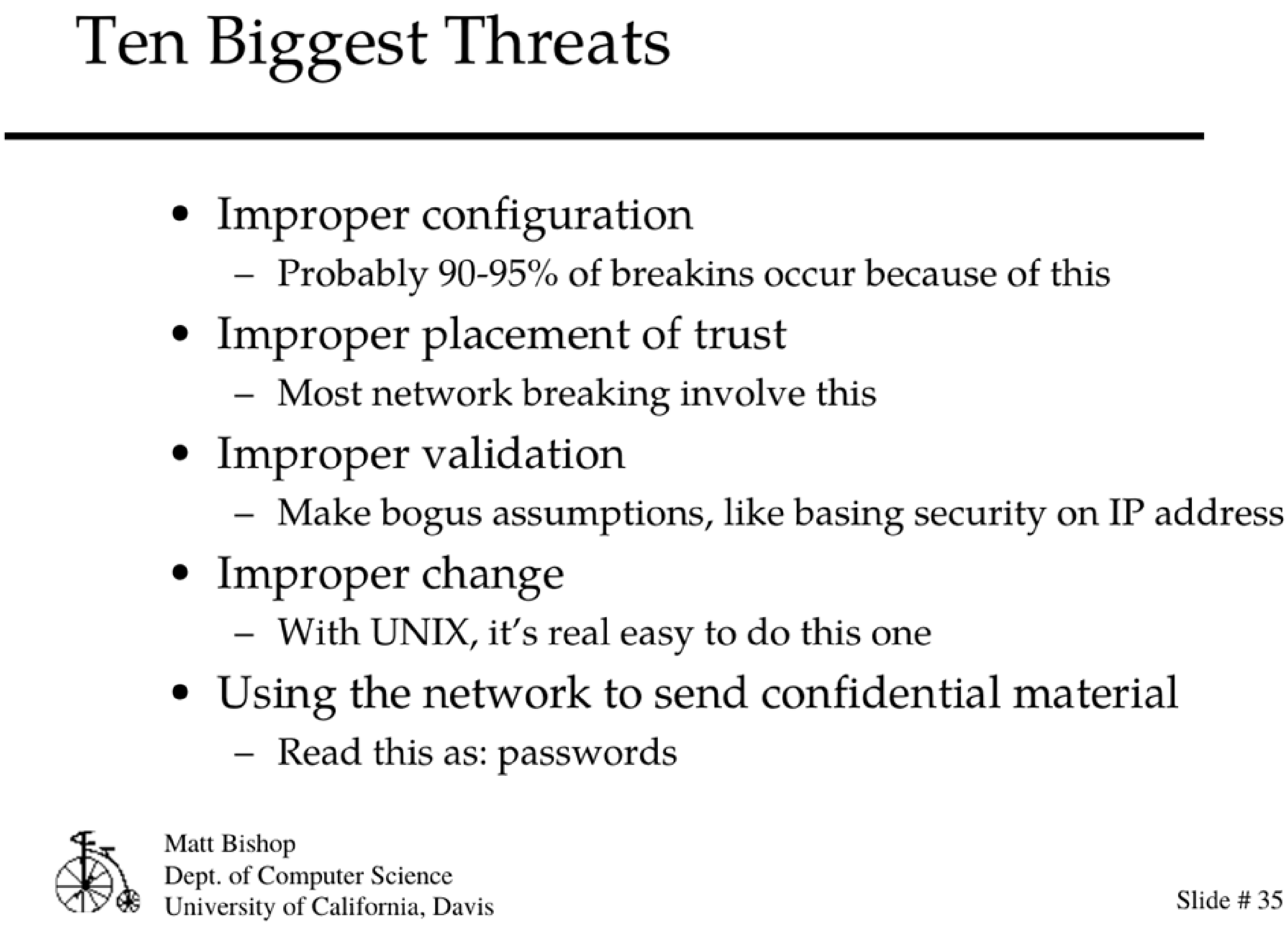
2. Real Word Examples 5

3. Social Engineering 11

4. Usable Security 12

5. Conclusion 15

# 1. Motivation



## Ten Biggest Threats

- Improper configuration
  - Probably 90-95% of breakins occur because of this
- Improper placement of trust
  - Most network breaking involve this
- Improper validation
  - Make bogus assumptions, like basing security on IP address
- Improper change
  - With UNIX, it's real easy to do this one
- Using the network to send confidential material
  - Read this as: passwords

Matt Bishop
Dept. of Computer Science
University of California, Davis

Slide # 35

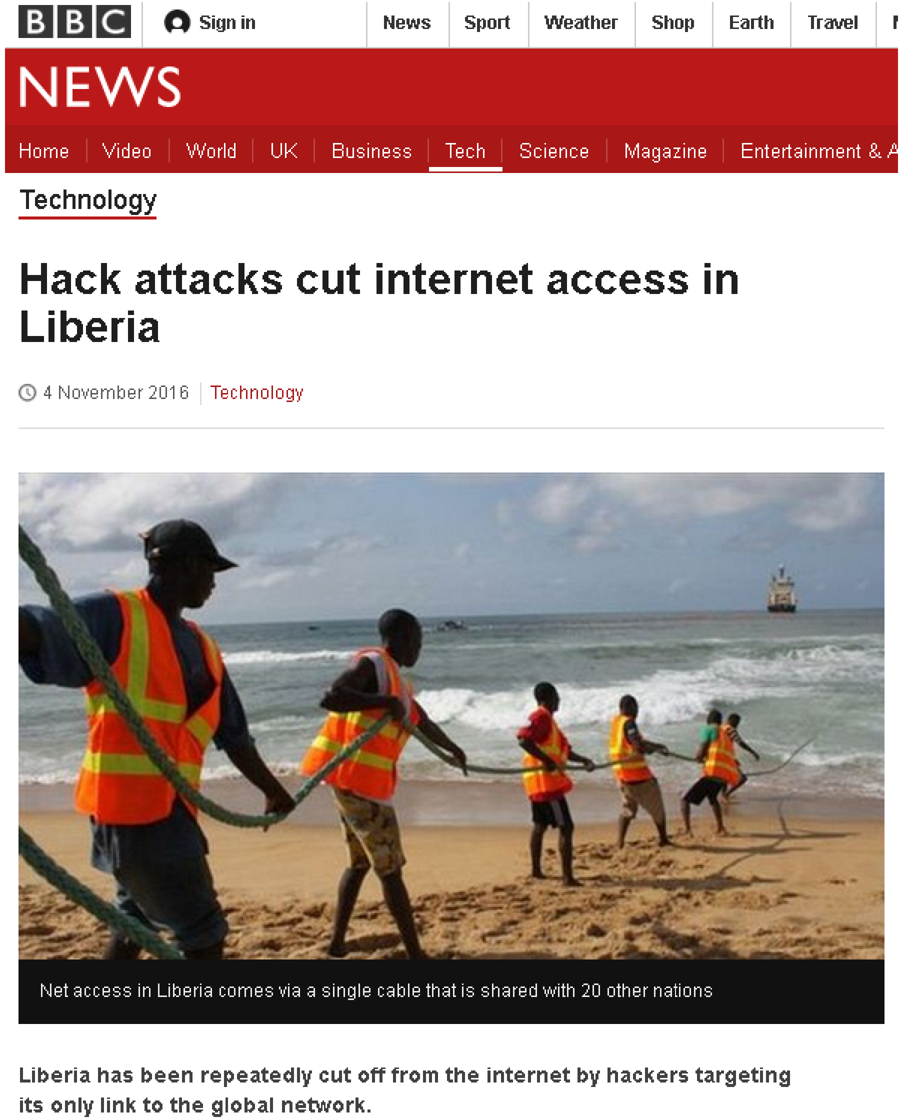
Matt Bishop, *UNIX Security: Threats and Solutions*, Presentation to SHARE 86.0, March 1996

# 2. Examples : Mirai (IoT-Botnet)

*“Recurrent attacks up to 3 November flooded the cable link with data, making net access intermittent.*

*Researchers said the attacks showed hackers trying different ways to use massive networks of hijacked machines to overwhelm high-value targets. (…)*

*A botnet variant called Mirai was identified by security firms as being the tool (…)”*



**Hack attacks cut internet access in Liberia**

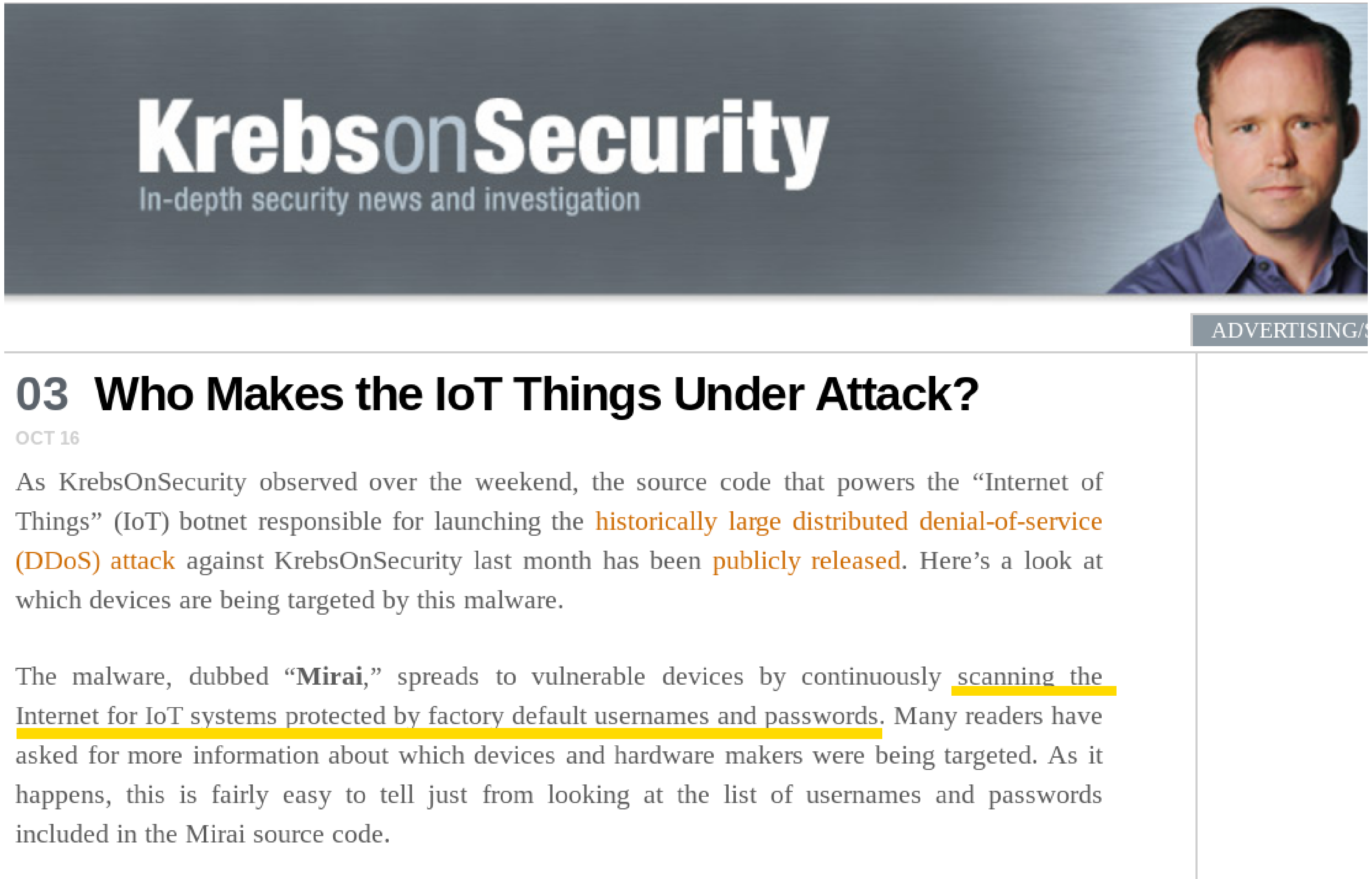
4 November 2016 | Technology

Net access in Liberia comes via a single cable that is shared with 20 other nations

**Liberia has been repeatedly cut off from the internet by hackers targeting its only link to the global network.**

BBC News: *Hack attacks cut internet access in Liberia*, www.bbc.com/news/technology-37859678, 2016-11-04

# 2. Examples: Mirai (IoT-Botnet)



## 03 Who Makes the IoT Things Under Attack?

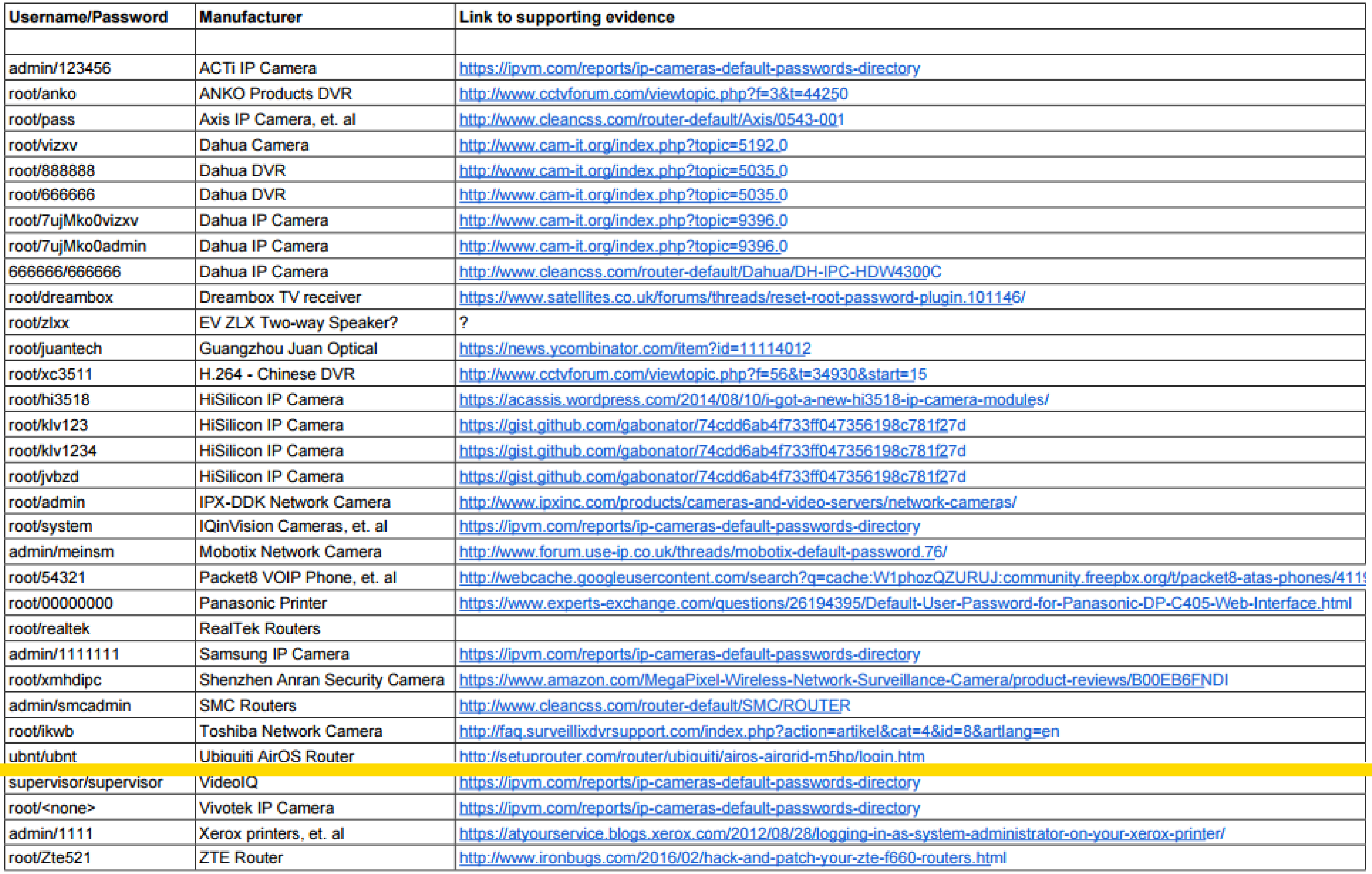
OCT 16

As KrebsOnSecurity observed over the weekend, the source code that powers the "Internet of Things" (IoT) botnet responsible for launching the historically large distributed denial-of-service (DDoS) attack against KrebsOnSecurity last month has been publicly released. Here's a look at which devices are being targeted by this malware.

The malware, dubbed "**Mirai**," spreads to vulnerable devices by continuously scanning the Internet for IoT systems protected by factory default usernames and passwords. Many readers have asked for more information about which devices and hardware makers were being targeted. As it happens, this is fairly easy to tell just from looking at the list of usernames and passwords included in the Mirai source code.

https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack

# 2. Examples: Mirai (IoT-Botnet)



| Username/Password | Manufacturer | Link to supporting evidence |
|---|---|---|
| | | |
| admin/123456 | ACTi IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/anko | ANKO Products DVR | http://www.cctvforum.com/viewtopic.php?f=3&t=44250 |
| root/pass | Axis IP Camera, et. al | http://www.cleancss.com/router-default/Axis/0543-001 |
| root/vizxv | Dahua Camera | http://www.cam-it.org/index.php?topic=5192.0 |
| root/888888 | Dahua DVR | http://www.cam-it.org/index.php?topic=5035.0 |
| root/666666 | Dahua DVR | http://www.cam-it.org/index.php?topic=5035.0 |
| root/7ujMko0vizxv | Dahua IP Camera | http://www.cam-it.org/index.php?topic=9396.0 |
| root/7ujMko0admin | Dahua IP Camera | http://www.cam-it.org/index.php?topic=9396.0 |
| 666666/666666 | Dahua IP Camera | http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C |
| root/dreambox | Dreambox TV receiver | https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/ |
| root/zlxx | EV ZLX Two-way Speaker? | ? |
| root/juantech | Guangzhou Juan Optical | https://news.ycombinator.com/item?id=11114012 |
| root/xc3511 | H.264 - Chinese DVR | http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15 |
| root/hi3518 | HiSilicon IP Camera | https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/ |
| root/klv123 | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/klv1234 | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/jvbzd | HiSilicon IP Camera | https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d |
| root/admin | IPX-DDK Network Camera | http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/ |
| root/system | IQinVision Cameras, et. al | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| admin/meinsm | Mobotix Network Camera | http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/ |
| root/54321 | Packet8 VOIP Phone, et. al | http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411 |
| root/00000000 | Panasonic Printer | https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html |
| root/realtek | RealTek Routers | |
| admin/1111111 | Samsung IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/xmhdipc | Shenzhen Anran Security Camera | https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI |
| admin/smcadmin | SMC Routers | http://www.cleancss.com/router-default/SMC/ROUTER |
| root/ikwb | Toshiba Network Camera | http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en |
| ubnt/ubnt | Ubiquiti AirOS Router | http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm |
| supervisor/supervisor | VideoIQ | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| root/<none> | Vivotek IP Camera | https://ipvm.com/reports/ip-cameras-default-passwords-directory |
| admin/1111 | Xerox printers, et. al | https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/ |
| root/Zte521 | ZTE Router | http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html |

https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack

# 2. Examples: Email Encryption

A. Whitten, J.D. Tygar:
*Why Johnny Can't Encrypt:  A Usability Evaluation of PGP 5.0,*
SSYM'99 Proceedings of the 8th conference on USENIX Security Symposium

PGP 5 Manual:
*"significantly improved graphical user interface makes complex mathematical cryptography accessible for  novice computer users"*

Lab study:

- 12 Participants, volunteers  in a political campaign
- Task: encrypt / decrypt / sign / verify
- Result:
  - Everything correct: **33%**
  - Secret transmitted in clear: **25 %**

Version 5.5
©1998 Network Associates, Inc. All rights reserved. PGP and Pretty Good Privacy are trademarks of Network Associates, Inc. All other trademarks are property of their respective holders. Export of this software may be restricted by the US government.

Image: PGP 5.5 Screenshot,
© Network Associates

# 2. Examples: Email Encryption

*„Digital Signing of messages is more problematic in PGP 9 than PGP 5 as none of the users were able to sign message using PGP-9”.*

S.Sheng, L.Broderick, C.A. Koranda, J.J. Hayland:
*Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software*,
SOUPS 2006

Mailvelope Logo,
Cornelis Norbertus Gysbrechts

*„(…) modern PGP tools are still unusable for the masses. (…)*

*We studied Mailvelope, a browser-based PGP (…) only one pair (out of 10) was able to successfully complete the assigned tasks(…)”*

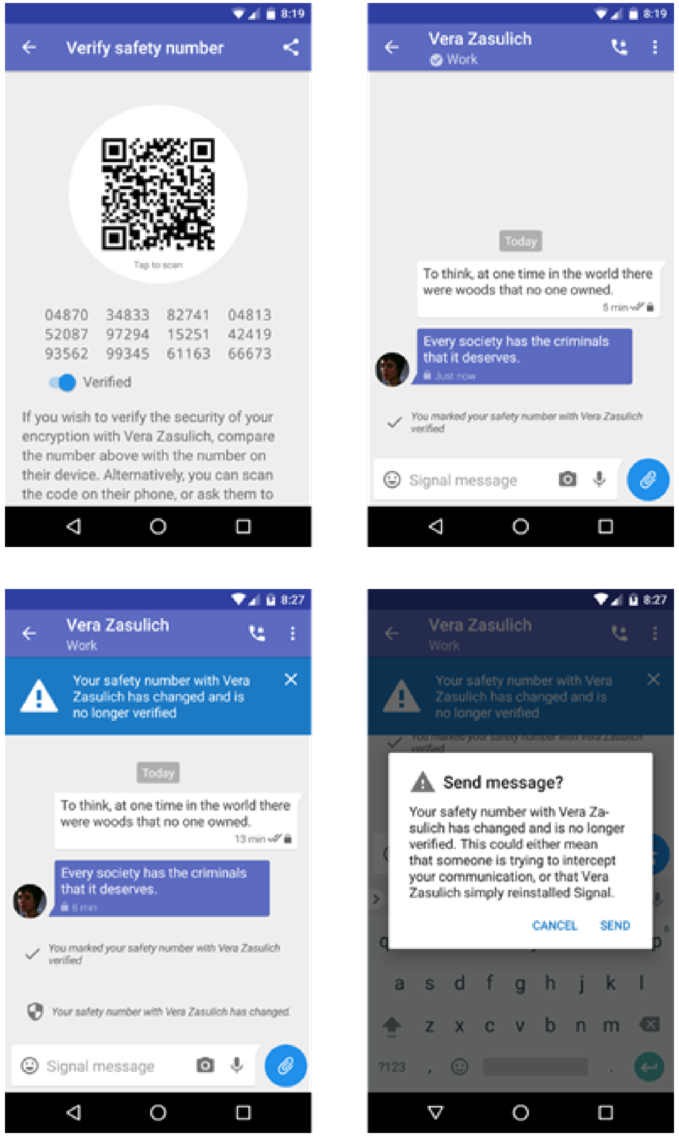
S.Ruoti, J. Andersen, D. Zappala, K.Seamons:
*Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client,*
SIGCHI 2015

# 2. Examples: Summary

1. Simple bugs
   - ISP Hardware: Default credentials
   - PGP 5: Emails sent unencrypted

2. How to avoid?
   - Employ an expert (?)
   - Structured Testing

3. Side constraint
   - Not a functional requirement / test case: “*Has to be secure*”
   - **What** to test?
   - **How** to test?



04870 34833 82741 04813
52087 97294 15251 42419
93562 99345 61163 66673

If you wish to verify the security of your encryption with Vera Zasulich, compare the number above with the number on their device. Alternatively, you can scan the code on their phone, or ask them to

To think, at one time in the world there were woods that no one owned.

Every society has the criminals that it deserves.

You marked your safety number with Vera Zasulich verified

Your safety number with Vera Zasulich has changed and is no longer verified

To think, at one time in the world there were woods that no one owned.

Every society has the criminals that it deserves.

You marked your safety number with Vera Zasulich verified

Your safety number with Vera Zasulich has changed.

Your safety number with Vera Zasulich has changed and is no longer verified

Send message?

Your safety number with Vera Zasulich has changed and is no longer verified. This could either mean that someone is trying to intercept your communication, or that Vera Zasulich simply reinstalled Signal.

Image: Open Whisper Systems Blog,
https://whispersystems.org/blog/verified-safety-number-updates/

# 3. Social Engineering: Intdocution

- It is even worse:

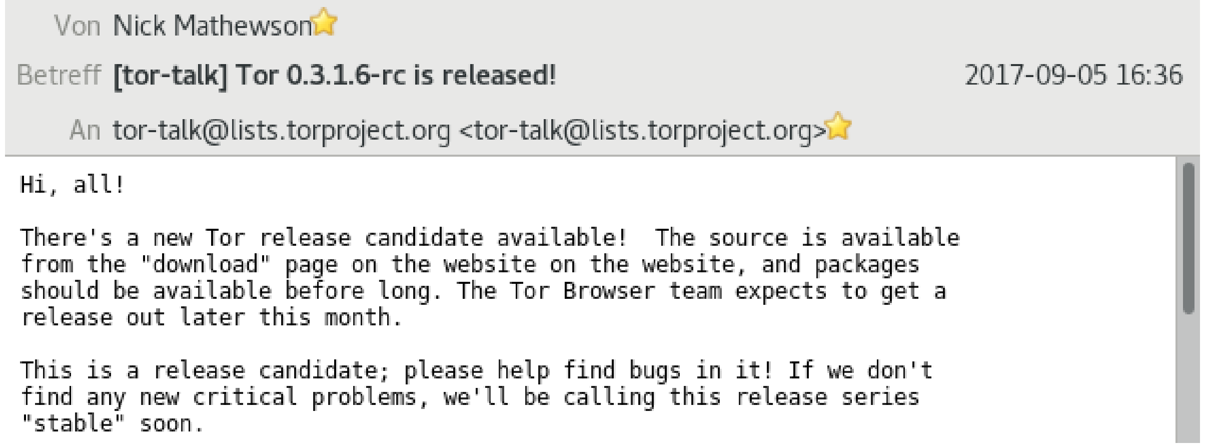
https://www.youtube.com/watch?v=lc7scxvKQOo

# 3. Social Engineering: Summary

- Target is made cooperative
  Bribery, blackmailing, persuasion (ethos, pathos, logos)

- Relation to usable privacy and security
  - Wrong understanding of outputs’ trustworthiness
  - Warnings / errors / bugs are expected
  - Users overwhelmed → Wrong decisions

- Goal: Resilient software
  - consistent, predictable, error-free
  - No illegal circumvention of security checks
  - Implications by 3rd party systems



Von Nick Mathewson

Betreff [tor-talk] Tor 0.3.1.6-rc is released! 2017-09-05 16:36

An tor-talk@lists.torproject.org <tor-talk@lists.torproject.org>

```
Hi, all!

There's a new Tor release candidate available!  The source is available
from the "download" page on the website on the website, and packages
should be available before long. The Tor Browser team expects to get a
release out later this month.

This is a release candidate; please help find bugs in it! If we don't
find any new critical problems, we'll be calling this release series
"stable" soon.
```

# 4. Usable Security

- What is Usability? (ISO 9241-11):
  “***The extent*** *to which*
  ***a product*** *can be used by*
  ***specified users*** *to achieve*
  ***specified goals*** *with*
  ***effectiveness****,* ***efficiency*** *and* ***satisfaction*** *in a specified* ***context*** *of use.”*

- Is ISO 9241-11 violated by PGP 5 ?

*“[..] Is this simply due to a failure to apply standard user interface design techniques to security?*

*We argue that, on the contrary, effective security requires a different usability standard, and that it* ***will not be achieved*** *through the user interface design techniques appropriate to other types of consumer software.”*

A. Whitten, J.D. Tygar: *Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0,*
SSYM'99 Proceedings of the 8th conference on USENIX Security Symposium

# 4. Usable Security: Criteria

**Security Software is usable, if users:**

1. Are reliably made aware of the security tasks they [..] perform
2. Are able to figure out how to successfully perform those [..]
3. Don’t make dangerous errors
4. Are sufficiently comfortable with the interface to continue using it.

**Problematic properties:**

1. The unmotivated user
2. The abstraction
3. The lack of feedback
4. The barn door
5. The weakest link

A. Whitten, J.D. Tygar: *Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0,* SSYM'99 Proceedings of the 8th conference on USENIX Security Symposium

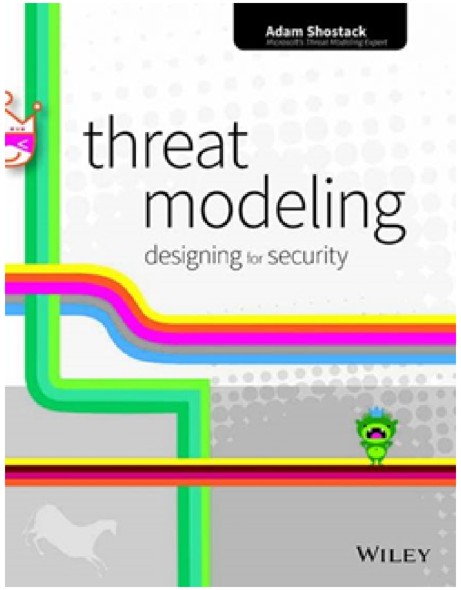
# 4. Achieving Usable Security

1. Designing for Usable Security
   - Design Persona (threat modelling)
   - Motivation via nudging, gamification

2. Do a product discovery phase
   - Cognitive walkthrough & think-aloud:
     Security expert: perception ok?

3. Usability as a criteria
   - Evaluate during user-acceptance-tests (UAT)
   - What is circumvented, ignored, etc. ?

4. Project methodology
   - It's not about clearance from security & UX anymore – it's about including them
   - Include test results & feedback: Agile is essential



# 5. Conclusion

1. **Security software is hard to use correctly**
   - ✓ Specific property
   - ✓ Security & privacy: part of all systems

2. **Privacy & security are usability aspects**
   - ✓ Include them during design and testing
   - ✓ Essential for achieving security
   - ✓ Social engineering:
     Taking advantage from missing usability
   - ✓ Classical usability is not enough

3. **When developing secure systems**
   - ✓ Evaluation results → changes in requirements
   - ✓ Test early and often → short cycles
   - ✓ Agile project management is essential
   - ✓ Include security and ux departments as early as possible

Tony Wills - CC-BY 2.5
https://en.wikipedia.org/wiki/Childproofing#/media/File:Child_proof_fence.jpg

Jan Lühr

anderScore GmbH

www.anderscore.com

jan.luehr@anderscore.c

TOPCONF Duesseldorf

anderScore trust in competence