Radboud University

Long-term security for the IoT?

Peter Schwabe
peter@cryptojedi.org
https://cryptojedi.org

November 6, 2017

Part I: The crypto nerd's imagination

https://xkcd.com/538/

"Make strong crypto run on small devices"

Crypto for the IoT

"Make strong crypto run on small devices"

- Lightweight Tweakable Block Ciphers

Crypto for the IoT

"Make strong crypto run on small devices"

- Lightweight Tweakable Block Ciphers
- Public-Key Cryptography on IoT Devices

Crypto for the IoT

"Make strong crypto run on small devices"

- Lightweight Tweakable Block Ciphers
- Public-Key Cryptography on IoT Devices
- RNGs for Resource-Constrained Devices

Crypto for the IoT

"Make strong crypto run on small devices"

- Lightweight Tweakable Block Ciphers
- Public-Key Cryptography on IoT Devices
- RNGs for Resource-Constrained Devices
- Lattice-based Cryptography for Embedded Devices

Crypto for the IoT

"Make strong crypto run on small devices"

- Lightweight Tweakable Block Ciphers
- Public-Key Cryptography on IoT Devices
- RNGs for Resource-Constrained Devices
- Lattice-based Cryptography for Embedded Devices

"Make strong crypto run on small devices"

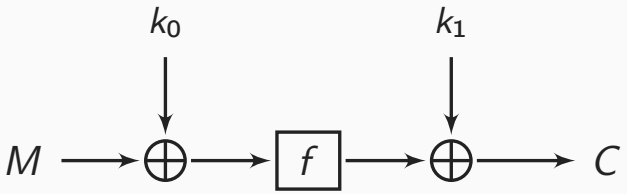
- Lightweight Tweakable Block Ciphers
- Public-Key Cryptography on IoT Devices
- RNGs for Resource-Constrained Devices
- Lattice-based Cryptography for Embedded Devices
- **Gimli: a cross-platform permutation.** Joint work with Daniel J. Bernstein, Stefan Kölbl, Stefan Lucks, Pedro Maat Costa Massolino, Florian Mendel, Kashif Nawaz, Tobias Schneider, François-Xavier Standaert, Yosuke Todo, and Benoît Viguier

Permutation-based crypto

"A permutation is a block cipher without a key"

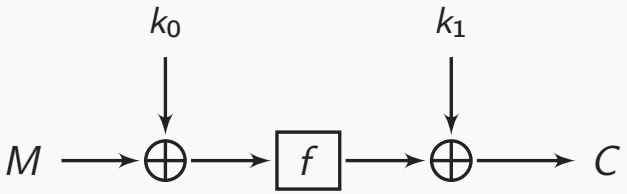
"A permutation is a block cipher without a key"

Even-Mansour construction

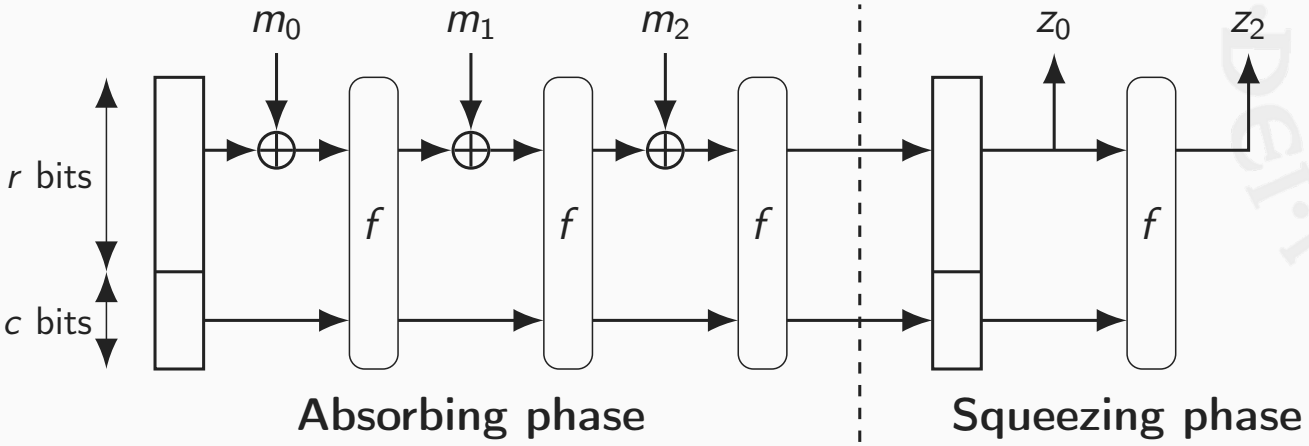


"A permutation is a block cipher without a key"

Even-Mansour construction



Sponge construction



Gimli: a 384-bit cross-platform permutation

- 384 bits = 12 32-bit words
- Fits into 14 32-bit integer registers on ARM Cortex-M
- Leaves 128-bit rate with 256-bit capacity for sponge
- Multiple of 128: good for NEON/SSE vectorization

Gimli: a 384-bit cross-platform permutation

- 384 bits = 12 32-bit words
- Fits into 14 32-bit integer registers on ARM Cortex-M
- Leaves 128-bit rate with 256-bit capacity for sponge
- Multiple of 128: good for NEON/SSE vectorization
- Arrange as 3×4 state matrix
- 3-bit bitsliced S-box operates on columns
- Instruction-level parallelism even for $128\times$ parallel S-box

Gimli: a 384-bit cross-platform permutation

- 384 bits = 12 32-bit words
- Fits into 14 32-bit integer registers on ARM Cortex-M
- Leaves 128-bit rate with 256-bit capacity for sponge
- Multiple of 128: good for NEON/SSE vectorization
- Arrange as 3×4 state matrix
- 3-bit bitsliced S-box operates on columns
- Instruction-level parallelism even for $128\times$ parallel S-box
- "Lightweight" diffusion across quarter states:
  - Work for long time on 96-bit quarter state
  - Reduce loads/stores on 8-bit AVR
  - Reduce vector-permute instructions on NEON and SSE/AVX

Gimli: a 384-bit cross-platform permutation

- 384 bits = 12 32-bit words
- Fits into 14 32-bit integer registers on ARM Cortex-M
- Leaves 128-bit rate with 256-bit capacity for sponge
- Multiple of 128: good for NEON/SSE vectorization
- Arrange as 3×4 state matrix
- 3-bit bitsliced S-box operates on columns
- Instruction-level parallelism even for $128\times$ parallel S-box
- "Lightweight" diffusion across quarter states:
  - Work for long time on 96-bit quarter state
  - Reduce loads/stores on 8-bit AVR
  - Reduce vector-permute instructions on NEON and SSE/AVX
- No ARX: enable efficient masking

Gimli in C

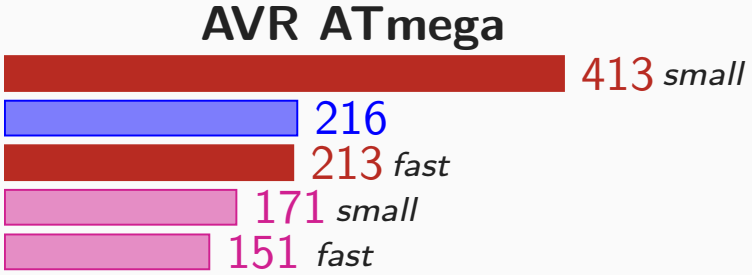
```c
void Gimli(uint32_t *state)
{
  uint32_t round, column, x, y, z;

  for (round = 24; round > 0; --round)
  {
    for (column = 0; column < 4; ++column)
    {
      x = rotate(state[    column], 24);                    // x <<< 24
      y = rotate(state[4 + column],  9);                    // y <<< 9
      z =        state[8 + column];
      state[8 + column] = x ^ (z << 1) ^ ((y & z) << 2);
      state[4 + column] = y ^ x        ^ ((x | z) << 1);
      state[column]     = z ^ y        ^ ((x & y) << 3);
    }
    if ((round & 3) == 0) { // small swap: pattern s...s...s... etc.
      x = state[0]; state[0] = state[1]; state[1] = x;
      x = state[2]; state[2] = state[3]; state[3] = x;
    }
    if ((round & 3) == 2) { // big swap: pattern ..S...S...S. etc.
      x = state[0]; state[0] = state[2]; state[2] = x;
      x = state[1]; state[1] = state[3]; state[3] = x;
    }
    if ((round & 3) == 0) { // add constant: pattern c...c...c... etc.
      state[0] ^= (0x9e377900 | round);
    }
  }
}
```

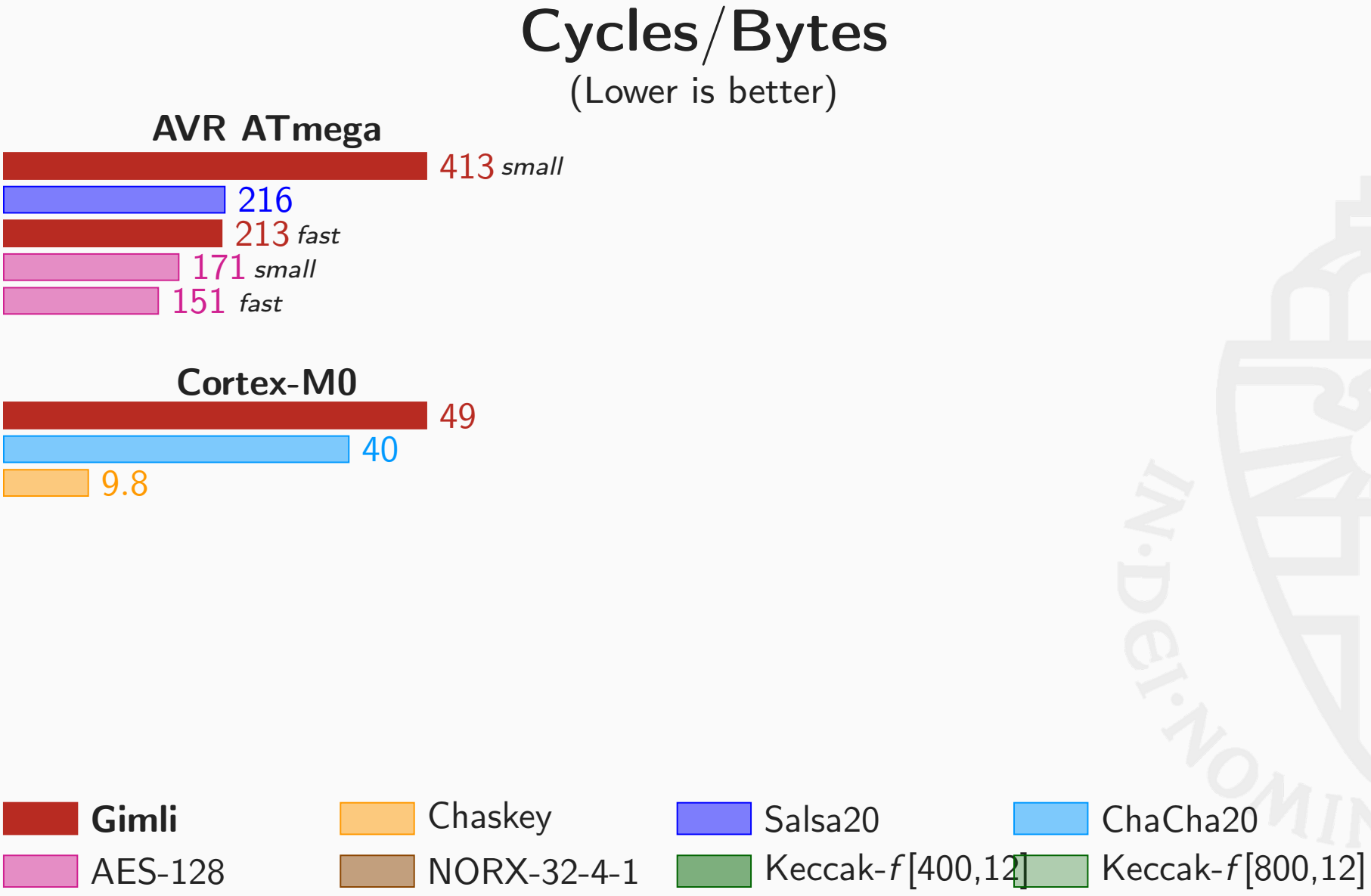
How fast is Gimli? (Software)

Cycles/Bytes

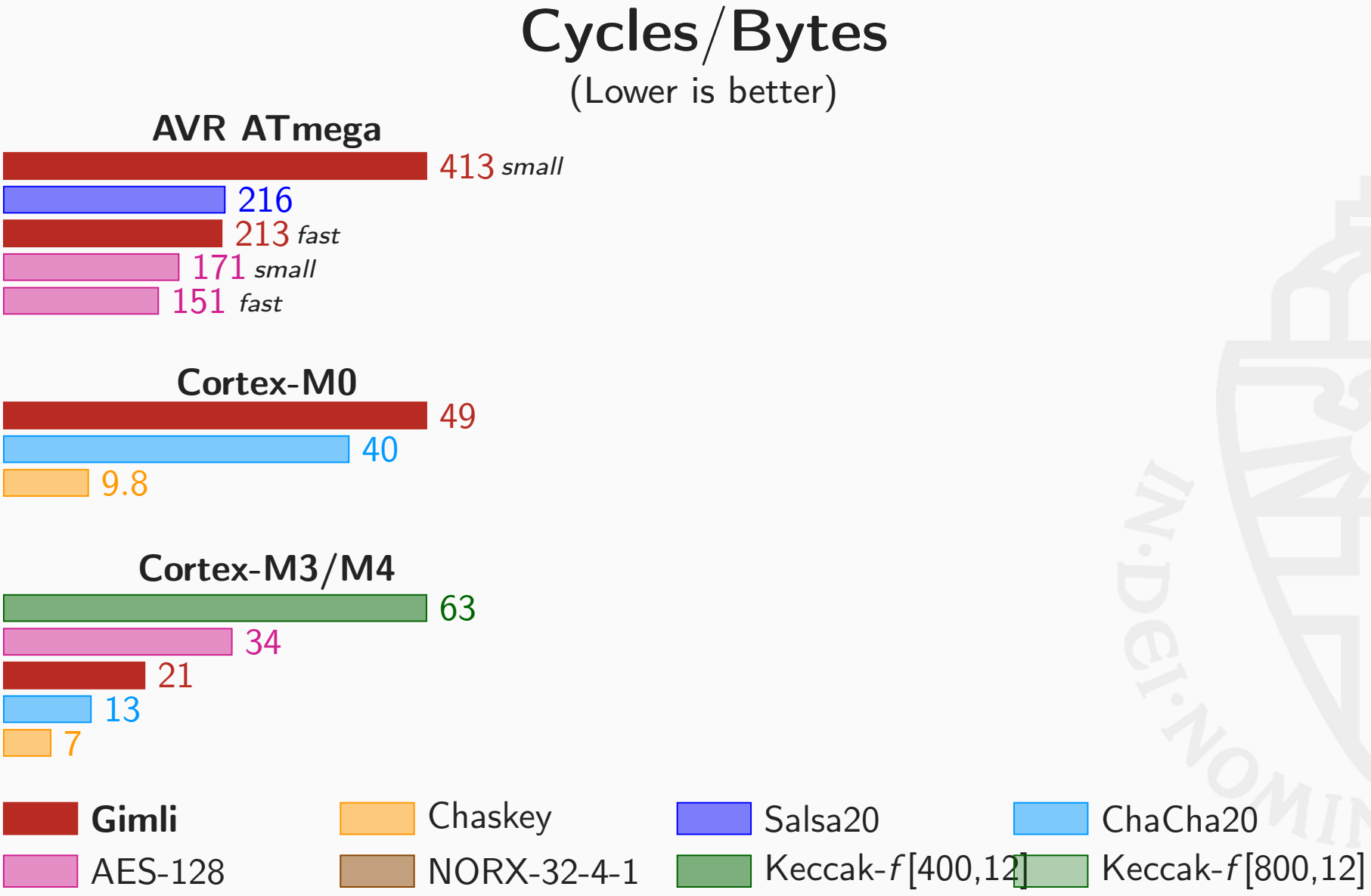
(Lower is better)



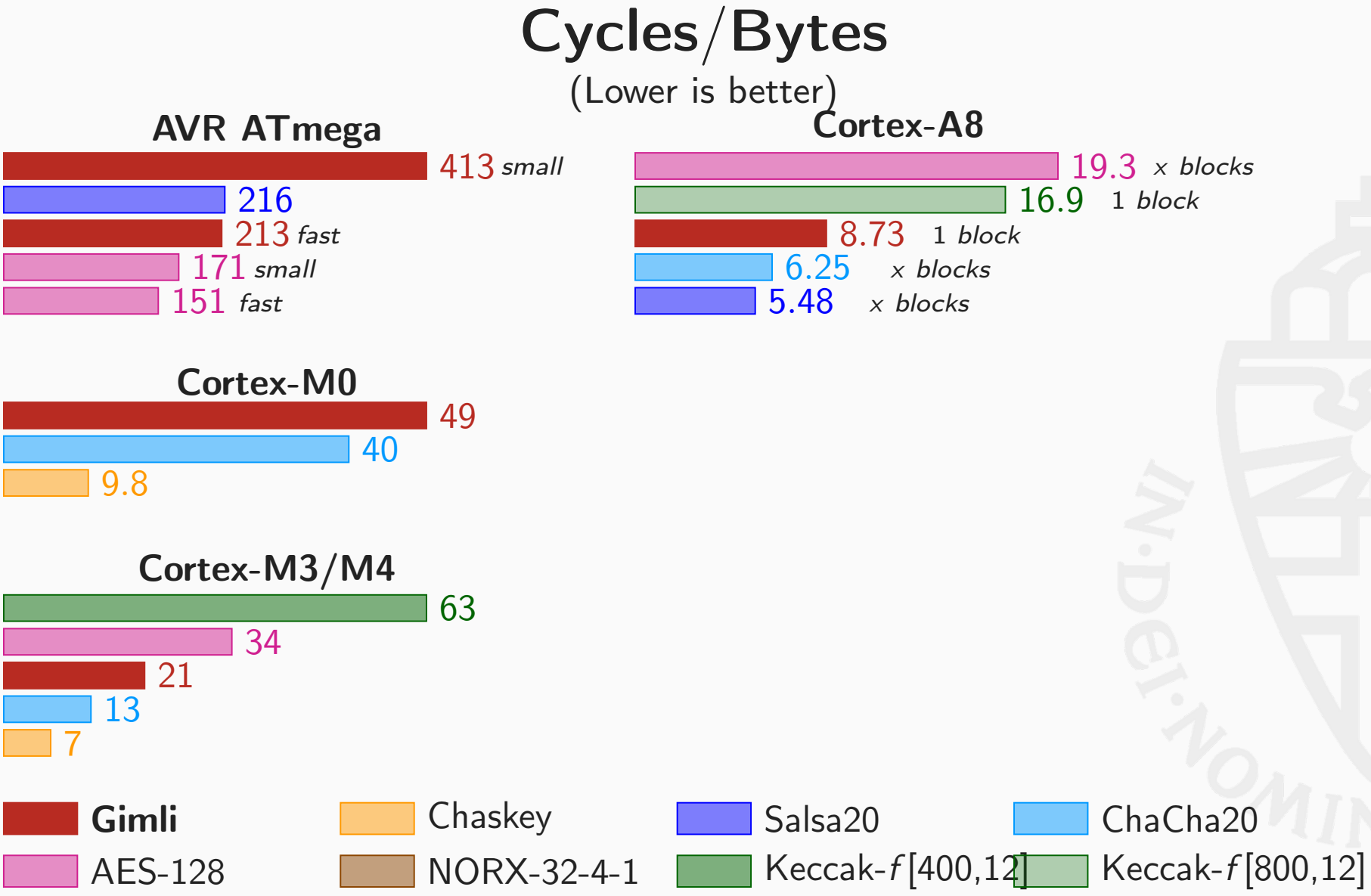
How fast is Gimli? (Software)



How fast is Gimli? (Software)



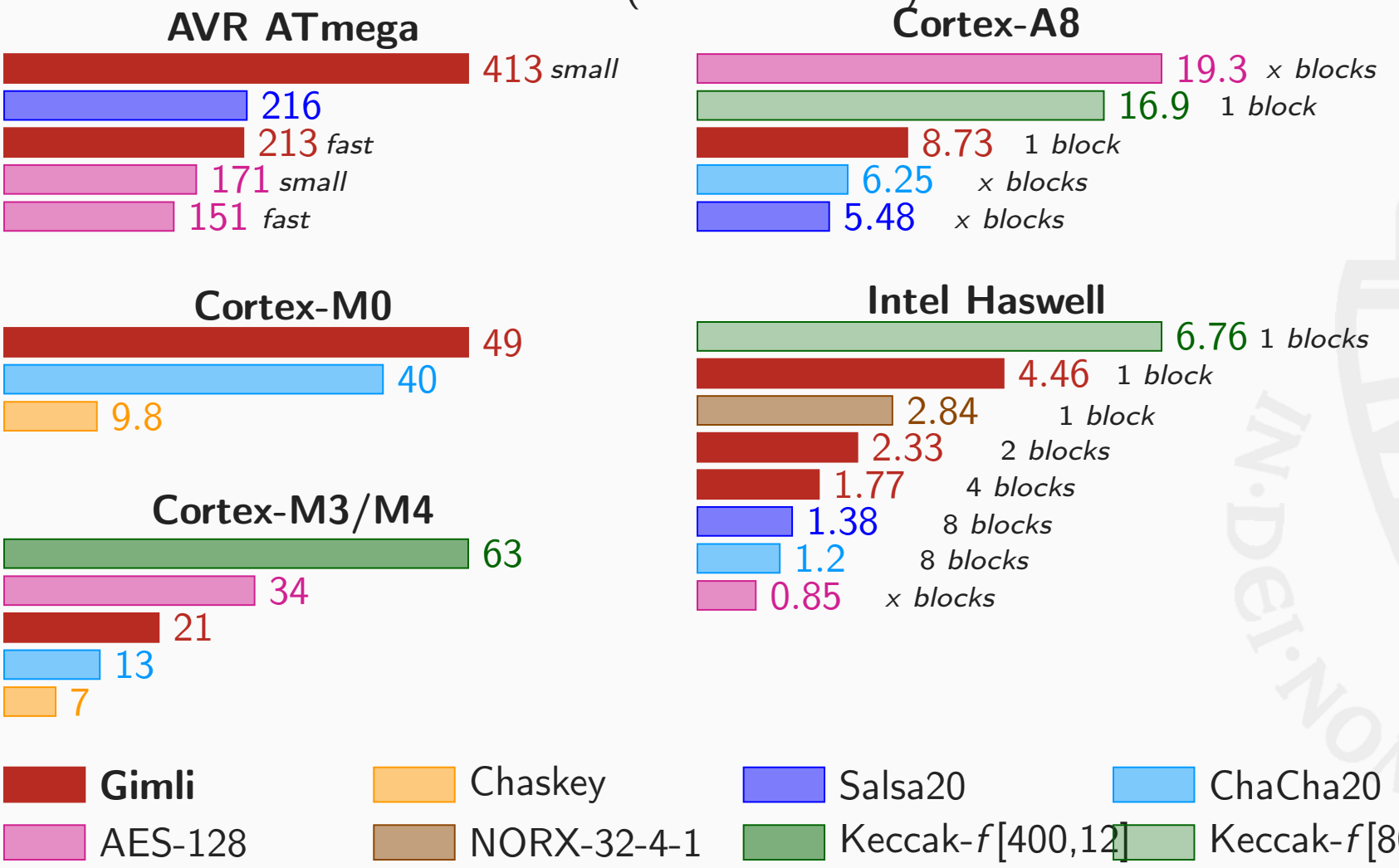
How fast is Gimli? (Software)



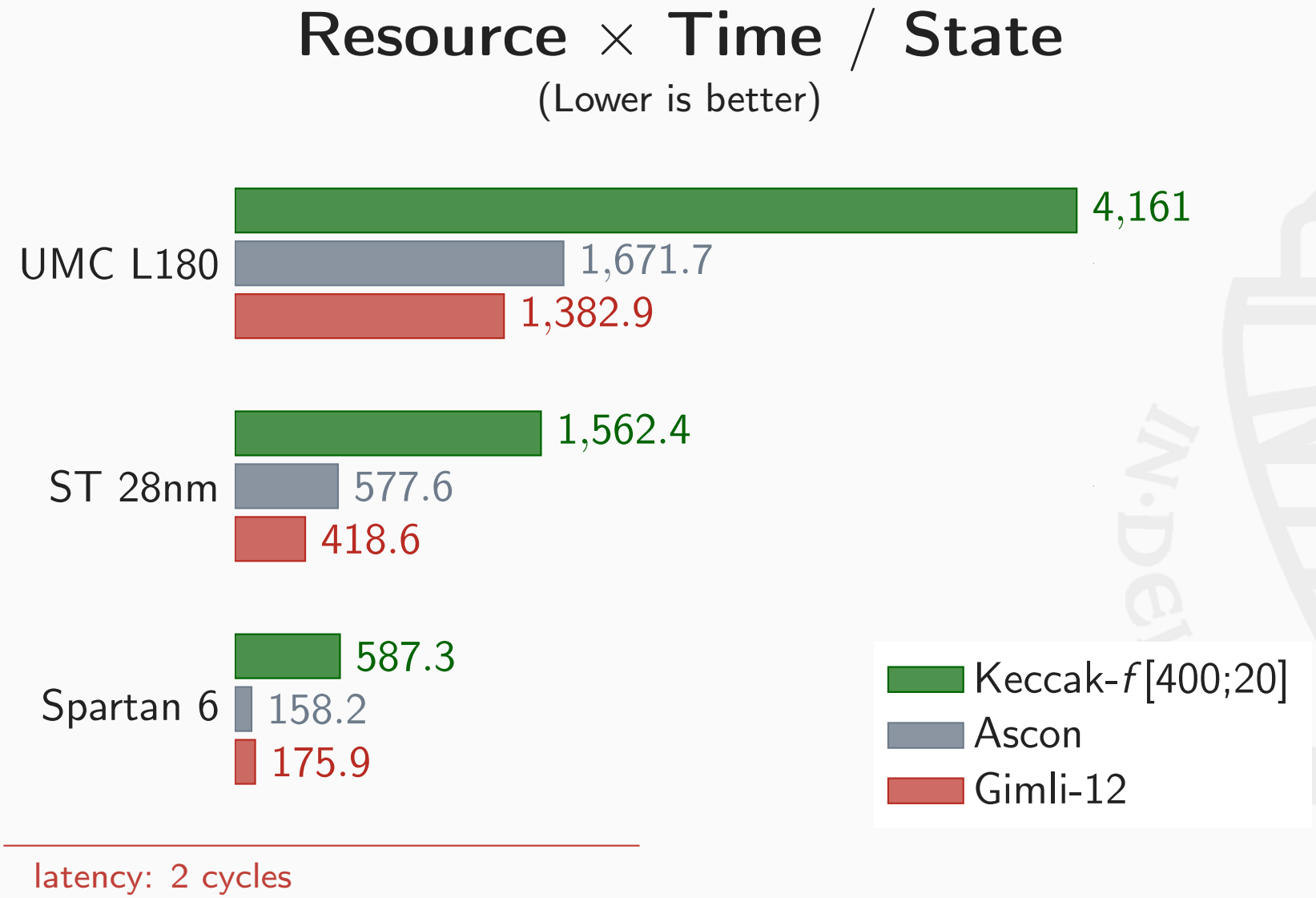
How fast is Gimli? (Software)

Cycles/Bytes

(Lower is better)



How efficient is Gimli? (Hardware)



How secure is Gimli?

- Avalanche effect for each state bit after 10 rounds
- Influence from each to each bit after 8 rounds
- Optimal differential trail for 8 rounds with prob. 2^{-52}
- Paper also includes some analysis for > 8 rounds

How secure is Gimli?

- Avalanche effect for each state bit after 10 rounds
- Influence from each to each bit after 8 rounds
- Optimal differential trail for 8 rounds with prob. 2^{-52}
- Paper also includes some analysis for > 8 rounds
- Hamburg, Aug 2017: Attack against 22.5 rounds
  - Exploits slow diffusion strategy of Gimli
  - Requires somewhat artificial mode of operation
  - Takes $2^{138.5}$ ops and 2^{129} mem
  - More expensive than 2^{192} brute force in real world
  - See statement at http://gimli.cr.yp.to/statement.html

How secure is Gimli?

- Avalanche effect for each state bit after 10 rounds
- Influence from each to each bit after 8 rounds
- Optimal differential trail for 8 rounds with prob. 2^{-52}
- Paper also includes some analysis for > 8 rounds
- Hamburg, Aug 2017: Attack against 22.5 rounds
  - Exploits slow diffusion strategy of Gimli
  - Requires somewhat artificial mode of operation
  - Takes $2^{138.5}$ ops and 2^{129} mem
  - More expensive than 2^{192} brute force in real world
  - See statement at http://gimli.cr.yp.to/statement.html
- Looking forward to more cryptanalysis of Gimli!

Gimli online

https://gimli.cr.yp.to

Part II: Reality

https://xkcd.com/538/

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"*

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"* Well, that's what you have to pay.

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"* Well, that's what you have to pay.
- *"We want lightweight crypto!"*

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"* Well, that's what you have to pay.
- *"We want lightweight crypto!"* You really want a stamp of approval on something cheaper than AES.

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"* Well, that's what you have to pay.
- *"We want lightweight crypto!"* You really want a stamp of approval on something cheaper than AES.
- *"256-bit ECC is way too expensive"*:

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"* Well, that's what you have to pay.
- *"We want lightweight crypto!"* You really want a stamp of approval on something cheaper than AES.
- *"256-bit ECC is way too expensive"*:
  - Can you design your protocol without asym. crypto? Great!

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"* Well, that's what you have to pay.
- *"We want lightweight crypto!"* You really want a stamp of approval on something cheaper than AES.
- *"256-bit ECC is way too expensive"*:
  - Can you design your protocol without asym. crypto? Great!
  - Do you need asym. crypto? It's not going to get cheaper than ECC.

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"* Well, that's what you have to pay.
- *"We want lightweight crypto!"* You really want a stamp of approval on something cheaper than AES.
- *"256-bit ECC is way too expensive"*:
  - Can you design your protocol without asym. crypto? Great!
  - Do you need asym. crypto? It's not going to get cheaper than ECC.
- *"I'm a researcher and want to do better than AES and 256-bit ECC!"*

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"* Well, that's what you have to pay.
- *"We want lightweight crypto!"* You really want a stamp of approval on something cheaper than AES.
- *"256-bit ECC is way too expensive"*:
  - Can you design your protocol without asym. crypto? Great!
  - Do you need asym. crypto? It's not going to get cheaper than ECC.
- *"I'm a researcher and want to do better than AES and 256-bit ECC!"*
  - Great, but that doesn't solve security problems of the IoT.

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"* Well, that's what you have to pay.
- *"We want lightweight crypto!"* You really want a stamp of approval on something cheaper than AES.
- *"256-bit ECC is way too expensive"*:
  - Can you design your protocol without asym. crypto? Great!
  - Do you need asym. crypto? It's not going to get cheaper than ECC.
- *"I'm a researcher and want to do better than AES and 256-bit ECC!"*
  - Great, but that doesn't solve security problems of the IoT.
- *"I'm a researcher and want to do post-quantum crypto"*

Crypto is not the problem

Solution to IoT crypto: Use AES and 256-bit ECC.

- *"AES is too expensive!"* Well, that's what you have to pay.
- *"We want lightweight crypto!"* You really want a stamp of approval on something cheaper than AES.
- *"256-bit ECC is way too expensive"*:
  - Can you design your protocol without asym. crypto? Great!
  - Do you need asym. crypto? It's not going to get cheaper than ECC.
- *"I'm a researcher and want to do better than AES and 256-bit ECC!"*
  - Great, but that doesn't solve security problems of the IoT.
- *"I'm a researcher and want to do post-quantum crypto"*
  - Great, but that doesn't solve security problems of the IoT.

Security

- Classical security issue:
  - Device gets compromised by attacker
  - Device does not behave as intended

Security

- Classical security issue:
  - Device gets compromised by attacker
  - Device does not behave as intended
- Not new, but much worse with IoT:
  - IoT devices from companies without security competence
  - Focus on functionality, UX, time-to-market

Security

- Classical security issue:
  - Device gets compromised by attacker
  - Device does not behave as intended
- Not new, but much worse with IoT:
  - IoT devices from companies without security competence
  - Focus on functionality, UX, time-to-market
  - Massive increase in devices $\Rightarrow$ massively larger botnets!
  - Direct impact on physical world (often safety critical)

Security

- Classical security issue:
  - Device gets compromised by attacker
  - Device does not behave as intended
- Not new, but much worse with IoT:
  - IoT devices from companies without security competence
  - Focus on functionality, UX, time-to-market
  - Massive increase in devices $\Rightarrow$ massively larger botnets!
  - Direct impact on physical world (often safety critical)
- Examples...

BUSINESS INSIDER NEDERLAND

INTERNATIONAAL

Akamai kicked journalist Brian Krebs' site off its servers after he was hit by a 'record' cyberattack

Paul Szoldra

22 Sep 2016 167

The cloud-hosting giant Akamai Technologies has dumped the website run by journalist Brian Krebs from its servers after the site came under a "record" cyberattack.

"It's looking likely that KrebsOnSecurity will be offline for a while," Krebs tweeted Thursday. "Akamai's kicking me off their network tonight."

Home Hacking Tech Deals Cyber Attacks Malware Spying

The Hacker News™
Security in a serious way

New Rapidly-Growing IoT Botnet Threatens to Take Down the Internet

Friday, October 20, 2017 Wang Wei

Tweet G+ Share Share 72 in Share Share Share

Security

REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

SMART HOME

Have a smart lock? Yeah, it can probably be hacked

Two security experts show just how easy it is to hack certain smart locks.

BY MEGAN WOLLERTON / AUGUST 9, 2016 3:43 PM PDT

Security

WIRED

Hackers Remotely Kill a Jeep on the Highway—With Me in It

BUSINESS | CULTURE | DESIGN | GEAR | SCIENCE | SECURITY

SHARE

SHARE

TWEET

COMMENT

EMAIL

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

There's a picture of Charlie and Chris in track suits

Availability

- IoT idea: Things with additional functionality via Internet

Availability

- IoT idea: Things with additional functionality via Internet
- IoT reality: Things with no functionality without Internet:

  My light switch didn't work because it was perpetually switched to the "on" position for Alexa to control the Philips smart lightbulb I had installed.

  I don't have a single regular lightbulb in my apartment. None of the light switches worked because they're all Wi-Fi-connected and controlled with Alexa.

  Reality finally sank in as a I realized my smart home, all piped through Alexa, had screwed me over and literally left me in the dark.

  —Raymond Wong

http://mashable.com/2016/07/05/smart-home-useless-internet-down/#8rp9Qs.tpkqK

Availability

- IoT idea: Things with additional functionality via Internet
- IoT reality: Things with no functionality without Internet:

  My light switch didn't work because it was perpetually switched to the "on" position for Alexa to control the Philips smart lightbulb I had installed.

  I don't have a single regular lightbulb in my apartment. None of the light switches worked because they're all Wi-Fi-connected and controlled with Alexa.

  Reality finally sank in as a I realized my smart home, all piped through Alexa, had screwed me over and literally left me in the dark.

  —Raymond Wong

  http://mashable.com/2016/07/05/smart-home-useless-internet-down/#8rp9Qs.tpkqK

- Similar issues for data in the cloud!

IoT Privacy – a nightmare

- Close to impossible to control what data is collected
- Close to impossible to control what data is sent
- Close to impossible to control what data is stored
- Close to impossible to control how data is sent and stored

IoT Privacy – a nightmare

c|net REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

SECURITY

Samsung's warning: Our Smart TVs record your living room chatter

Technically Incorrect: Samsung's small print says that its Smart TV's voice recognition system will not only capture your private conversations, but also pass them onto third parties.

BY CHRIS MATYSZCZYK / FEBRUARY 8, 2015 2:10 PM PST

IoT Privacy – a nightmare

sign in | become a supporter | subscribe | search | find a job | dating | more | International edition

theguardian

UK | world | sport | football | opinion | culture | business | lifestyle | fashion | environment | tech | travel | browse all sections

home › world › europe | US | americas | asia | australia | africa | middle east | cities | development

Germany

German parents told to destroy doll that can spy on children

German watchdog classifies My Friend Cayla doll as 'illegal espionage apparatus' and says shops and owners could face fines

This article is 9 months old

2,669

Philip Oltermann

@philipoltermann

Friday 17 February 2017 16.53 GMT

Jayla, aged four, plays with a My Friend Cayla doll in the Hamleys toy shop in London. Photograph: Rob Stothard/Getty Images

Most popular

Texas church shooting: suspect named as at least 26 confirmed dead – as it happened

Paradise Papers leak reveals secrets of the world elite's hidden wealth

Trump dump: president throws entire box of fish food into precious koi carp pond

Russia funded Facebook and Twitter investments

IoT Privacy – a nightmare

sign in | become a supporter | subscribe | search | find a job | dating | more | International edition

theguardian

UK | world | sport | football | opinion | culture | business | lifestyle | fashion | environment | tech | travel | browse all sections

home › tech

Data and computer security

Someone made a smart vibrator, so of course it got hacked

The We-Vibe 4 Plus is a vibrator with a computer inside it - but hackers say it also phones home, telling its makers when it's being used

This article is 1 year old

Alex Hern in San Francisco

@alexhern

Wednesday 10 August 2016 08.00 BST

Two hackers revealed that the way the vibrator speaks with its controlling app isn't really secure at all. Photograph: WeVibe

IoT Privacy – a nightmare

"Am Sonntagabend eröffnet die Bundeskanzlerin die CeBIT in Hannover. Bezogen auf den Automobilsektor sagte sie, es sei wichtig, ob die Daten dem Autohersteller oder dem Softwarehersteller gehörten."

https://heise.de/-3658576

Underlying problem

Nobody cares

- **Users** don't care if their camera attacks some webserver
- Many **users** care little about loss of privacy

Underlying problem

Nobody cares

- **Users** don't care if their camera attacks some webserver
- Many **users** care little about loss of privacy
- Primary goal of **industry** is not to build secure devices
- Primary goal of **industry** is to make money

Underlying problem

Nobody cares

- **Users** don't care if their camera attacks some webserver
- Many **users** care little about loss of privacy
- Primary goal of **industry** is not to build secure devices
- Primary goal of **industry** is to make money
- Nobody has to pay for damage caused by IoT devices
- Nobody has a (financial) interest in secure devices

Underlying problem

Nobody cares

- **Users** don't care if their camera attacks some webserver
- Many **users** care little about loss of privacy
- Primary goal of **industry** is not to build secure devices
- Primary goal of **industry** is to make money
- Nobody has to pay for damage caused by IoT devices
- Nobody has a (financial) interest in secure devices

Those who do, don't have a choice

- Smart meters are mandatory
- In NL, I cannot use public transportation without the OV Chipcard
- In a few years all (?) cars will support OTA updates
- You share public space with IoT devices you don't own
- You share private space with IoT devices you don't own

Bad solution: mandatory certification

Certification does not work

- Example 1: Bernstein, Chang, Cheng, Chou, Heninger, Lange, and van Someren 2013
  - RSA keys on Taiwanese citizen cards are terribly insecure
  - Those cards were "accredited to FIPS 140-1 level 2"

Bad solution: mandatory certification

Certification does not work

- Example 1: Bernstein, Chang, Cheng, Chou, Heninger, Lange, and van Someren 2013
  - RSA keys on Taiwanese citizen cards are terribly insecure
  - Those cards were "accredited to FIPS 140-1 level 2"
- Example 2: Nemec, Sys, Svenda, Klinec, and Matyas, 2017: ROCA
  - Infineon RSA key generation terribly insecure
  - Devices certified by FIPS 140-2 and CC EAL 5+

Bad solution: mandatory certification

Certification does not work

- Example 1: Bernstein, Chang, Cheng, Chou, Heninger, Lange, and van Someren 2013
  - RSA keys on Taiwanese citizen cards are terribly insecure
  - Those cards were "accredited to FIPS 140-1 level 2"
- Example 2: Nemec, Sys, Svenda, Klinec, and Matyas, 2017: ROCA
  - Infineon RSA key generation terribly insecure
  - Devices certified by FIPS 140-2 and CC EAL 5+
- The goal of certification is to divert responsibility

Bad solution: mandatory certification

Certification does not work

- Example 1: Bernstein, Chang, Cheng, Chou, Heninger, Lange, and van Someren 2013
  - RSA keys on Taiwanese citizen cards are terribly insecure
  - Those cards were "accredited to FIPS 140-1 level 2"
- Example 2: Nemec, Sys, Svenda, Klinec, and Matyas, 2017: ROCA
  - Infineon RSA key generation terribly insecure
  - Devices certified by FIPS 140-2 and CC EAL 5+
- The goal of certification is to divert responsibility
- "Well, maybe it still doesn't hurt"...

Bad solution: mandatory certification

Certification actively harms

- CC validation of smartcards: limit information about TOE
- Public evaluation of security becomes hard or impossible
- For long-term security we *need public research*

Bad solution: mandatory certification

Certification actively harms

- CC validation of smartcards: limit information about TOE
- Public evaluation of security becomes hard or impossible
- For long-term security we *need public research*
- Certified devices need re-certification for updates
- Fast updates are often critical for security
- Certification takes time and money

Solution (?): make someone care

Solution suggested (similarly) by Felix von Leitner
https://ptrace.fefe.de/iot/iot.html#6

- Make producers liable for damage caused by their IoT products

Solution (?): make someone care

Solution suggested (similarly) by Felix von Leitner
https://ptrace.fefe.de/iot/iot.html#6

- Make producers liable for damage caused by their IoT products
- Access to market only with adequate insurance

Solution (?): make someone care

Solution suggested (similarly) by Felix von Leitner
https://ptrace.fefe.de/iot/iot.html#6

- Make producers liable for damage caused by their IoT products
- Access to market only with adequate insurance
- Producers have to specify (reasonable) lifetime
- Producers have to guarantee lifetime support

Solution (?): make someone care

Solution suggested (similarly) by Felix von Leitner
https://ptrace.fefe.de/iot/iot.html#6

- Make producers liable for damage caused by their IoT products
- Access to market only with adequate insurance
- Producers have to specify (reasonable) lifetime
- Producers have to guarantee lifetime support
- Require privacy by design (incl. data minimization)

Solution (?): make someone care

Solution suggested (similarly) by Felix von Leitner
https://ptrace.fefe.de/iot/iot.html#6

- Make producers liable for damage caused by their IoT products
- Access to market only with adequate insurance
- Producers have to specify (reasonable) lifetime
- Producers have to guarantee lifetime support
- Require privacy by design (incl. data minimization)

⇒ **Make it expensive to sell insecure devices or to leak data**

Problem 1: Doesn't that destroy the market?

Problem 1: Doesn't that destroy the market?

Answer: Yes. So... problem solved.

Problem 1: Doesn't that destroy the market?

Devices with limited use

- Many IoT devices are not. . . well. . . overly useful
- You don't want botnets of hairbrushes and egg trays?
  - Make them more secure (see above)
  - This increases cost
  - This possibly makes UX worse

Problem 1: Doesn't that destroy the market?

Devices with limited use

- Many IoT devices are not. . . well. . . overly useful
- You don't want botnets of hairbrushes and egg trays?
  - Make them more secure (see above)
  - This increases cost
  - This possibly makes UX worse
- Two effects:
  - Higher prices, worse UX: fewer devices ⇒ less botnet potential
  - Harder to compromise ⇒ less botnet potential

Problem 1: Doesn't that destroy the market?

Devices with limited use

- Many IoT devices are not. . . well. . . overly useful
- You don't want botnets of hairbrushes and egg trays?
  - Make them more secure (see above)
  - This increases cost
  - This possibly makes UX worse
- Two effects:
  - Higher prices, worse UX: fewer devices ⇒ less botnet potential
  - Harder to compromise ⇒ less botnet potential
- Compare to tobacco market:
  - Politics recognized harm to consumers and bystanders
  - Politics increased prices and made UX worse
  - Fewer people smoke ⇒ less harm

Problem 1: Doesn't that destroy the market?

Devices with *actual* benefit

- Benefit for the producer (example: OTA car updates): producer is willing to pay
- Benefit for the user (example: surveillance camera): user is willing to pay
- Benefit for society (example: smart meters): politics is willing to (make people) pay
- Cost increases for every market participant

Problem 2: updating IoT devices

- IoT devices won't be "perfectly secure" (at least for some time)
- Typical answer: security updates

Problem 2: updating IoT devices

- IoT devices won't be "perfectly secure" (at least for some time)
- Typical answer: security updates
- For smartphones and computers can involve user
- For IoT devices kind of need auto updates

Problem 2: updating IoT devices

- IoT devices won't be "perfectly secure" (at least for some time)
- Typical answer: security updates
- For smartphones and computers can involve user
- For IoT devices kind of need auto updates
- Do you want to give producers a remote-control to your device?
- Do you want additional security issues from updates?

Problem 3: user's responsibility

- Are users becoming liable for damage caused after "lifetime"?
- What happens if users change the firmware?
- Need insurance for running Linux?

Problem 4: the IoT is not tobacco

English | En Français

allAfrica

Se

BY ALLAFRICA | NEWS SO

Countries | Topics | Development | BizTech | Entertainment | Sport | Africa/World | Governance | Multimedia | Innovatic

AfricaFocus

9 OCTOBER 2017

Africa: Tobacco Industry Targets Africa Markets

Tagged: Africa • Business • Company • Health • NCDs

Photo: Premium Times

(File photo).

ANALYSIS

"British American Tobacco (BAT) and other multinational tobacco firms have threatened governments in at least eight countries in Africa demanding they axe or dilute the

MORE ON THIS

Tobacco Industry Targets African Markets

WHO Rejects Philip Morris' Anti-Smoking Foundation

Cigarette Manufacturer

MORE FROM: AFRIC

Africa: Recent Books Re

Africa: Not Only a Somal

Africa: Tobacco Industry Markets

Africa: Africa/Global - Ho Tax Injustice

Sierra Leone: Sierra Leo From Disaster

Africa: Does Trump's Adr

RELATED

Problem 4: the IoT is not tobacco

- Europe can (maybe) control the EU market
- Vendors/producers will escape to other markets
- For tobacco: "somebody elses problem"
- For IoT devices: **Still our problem**
- You don't care where the crappy IoT devices are that attack your webserver!

Summary

- IoT security is primarily a political and legal problem
- Technical issues are challenging, but secondary
- Crypto issues are at most ternary

Credit

Slides inspired by

- Felix von Leitner's IoT talk:
  https://ptrace.fefe.de/iot/iot.html#6
- @internetofshit
- Troy Hunt: "What Would It Look Like If We Put Warnings on IoT Devices Like We Do Cigarette Packets?"
  http://tinyurl.com/y83qh988