An easy attack on AEZ

Xavier Bonnetain Patrick Derbez Sébastien Duval Jérémy Jean
Gaëtan Leurent Brice Minaud Valentin Suder

FSE 2017 Rump Session

Cryptograpy for the Internet of Things

- Lightweight cryptograpy is required for the IoT
- Here is a concrete example:
- Toilet in my hotel is remote controlled!
- Some models use Bluetooth!
- Important confidentiality and authenticity issues!
- Man in the 🚽 attack!
- Denial of 💩 attack!
- Targeted attacks: 

- Welcome to the Internet of 💩!

Cryptograpy for the Internet of Things

- Lightweight cryptograpy is required for the IoT
- Here is a concrete example:
- Toilet in my hotel is remote controlled!
- Some models use Bluetooth!
- Important confidentiality and authenticity issues!
- Man in the 🚽 attack!
- Denial of 💩 attack!
- Targeted attacks: 
- Welcome to the Internet of 💩!

Cryptograpy for the Internet of Things

- Lightweight cryptograpy is required for the IoT
- Here is a concrete example:
- Toilet in my hotel is remote controlled!
- Some models use Bluetooth!
- Important confidentiality and authenticity issues!
- Man in the 🚽 attack!
- Denial of 💩 attack!
- Targeted attacks: 
- Welcome to the Internet of 💩!

Cryptograpy for the Internet of Things

- Lightweight cryptograpy is required for the IoT
- Here is a concrete example:
- Toilet in my hotel is remote controlled!
- Some models use Bluetooth!
- Important confidentiality and authenticity issues!
- Man in the 🚽 attack!
- Denial of 💩 attack!
- Targeted attacks: 

- Welcome to the Internet of 💩!

Cryptograpy for the Internet of Things

- Lightweight cryptograpy is required for the IoT
- Here is a concrete example:
- Toilet in my hotel is remote controlled!
- Some models use Bluetooth!
- Important confidentiality and authenticity issues!
- Man in the 🚽 attack!
- Denial of 💩 attack!
- Targeted attacks: 
- Welcome to the Internet of 💩!

Cryptograpy for the Internet of Things

- Lightweight cryptograpy is required for the IoT
- Here is a concrete example:
- Toilet in my hotel is remote controlled!
- Some models use Bluetooth!
- Important confidentiality and authenticity issues!
- Man in the 🚽 attack!
- Denial of 💩 attack!
- Targeted attacks: 

- Welcome to the Internet of 💩!

Cryptograpy for the Internet of Things

- Lightweight cryptograpy is required for the IoT

- Here is a concrete example:

- Toilet in my hotel is remote controlled!
- Some models use Bluetooth!

- Important confidentiality and authenticity issues!
- Man in the 🚽 attack!
- Denial of 💩 attack!
- Targeted attacks: 

- Welcome to the Internet of 💩!

Cryptograpy for the Internet of Things

- Lightweight cryptograpy is required for the IoT

- Here is a concrete example:

- Toilet in my hotel is remote controlled!
- Some models use Bluetooth!

- Important confidentiality and authenticity issues!
- Man in the 🚽 attack!
- Denial of 💩 attack!
- Targeted attacks: 

- Welcome to the Internet of 💩!

Cryptograpy for the Internet of Thi

- Lightweight cryptog
-
-
- S
- In
  au
- Ma
- Der
- Targ
- Welc nternet of 💩!

How smart toilet in Japan became prone to hacking

Brett Molina, USA TODAY Published 9:59 a.m. ET Aug. 6, 2013 | Updated 10:16 a.m. ET Aug. 6, 2013

416 CONNECT TWEET LINKEDIN 3 COMMENT EMAIL MORE

(Photo: Getty Images)

Not even the porcelain throne is safe from a potential hacking.

Security company Trustwave issued an advisory to owners of the Satis smart toilet, currently available in Japan, which pairs with a Google Android app through Bluetooth.

Thanks to a vulnerability within the app, Trustwave says any person could download the My Satis app and gain control of any Satis smart toilet.

So, what potty peril could a Satis toilet owner discover? Trustwave says users could repeatedly flush the toilet, driving up water costs, or remotely open and close the toilet lid as well as activate the bidet, "causing discomfort or distress to (the) user."

The company says Satis makers Lixil have yet to respond to the security issue.

According to a Satis brochure, the toilet features multiple cleansing options, heated seat and even plays music. NPR notes the Satis app allows users to control the commode and keep track of their bathroom activity.

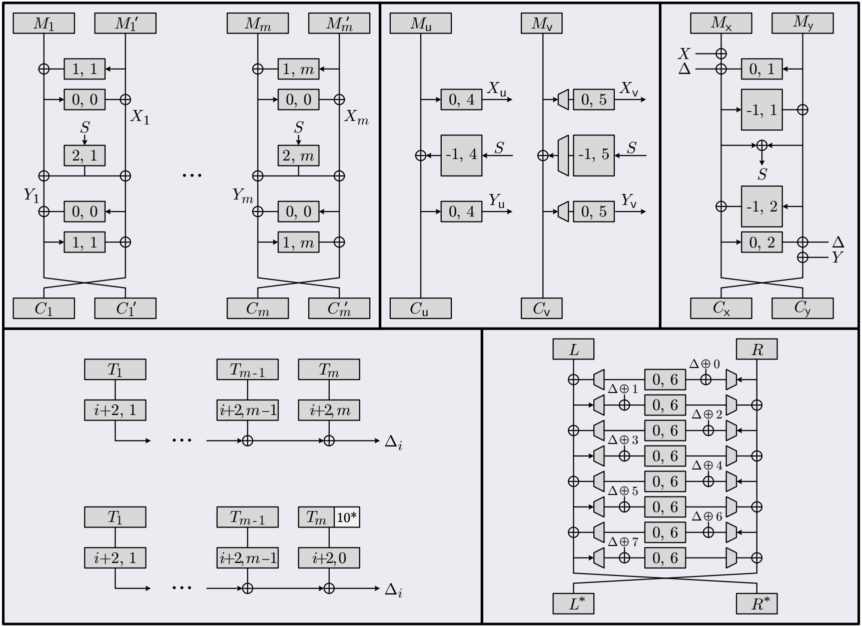
This isn't the first case of a smart technology prone to shenanigans from curious Internet users. Last month, a Forbes writer detailed how she was able to gain easy access to home automation systems.

AEZ

Viet Tung Hoang, Ted Krovetz & Phillip Rogaway
Robust Authenticated-Encryption
AEZ and the Problem That It Solves
EUROCRYPT 2015

- Very strong security goal: robust authenticated encryption
- Very complex design: huge state, many subcases

- Third round CAESAR candidate
- Tor is considering using AEZ



M1 M1′ Mm Mm′
1, 1
0, 0
X1
S
2, 1
Y1
0, 0
1, 1
1, m
0, 0
Xm
S
2, m
Ym
0, 0
1, m
C1 C1′ Cm Cm′
Mu Mv
0, 4 Xu
-1, 4 S
0, 4 Yu
0, 5 Xv
-1, 5 S
0, 5 Yv
Cu Cv
Mx My
X
Δ
0, 1
-1, 1
S
-1, 2
0, 2
Δ
Y
Cx Cy
T1 Tm-1 Tm
i+2, 1
i+2, m−1
i+2, m
Δi
T1 Tm-1 Tm 10*
i+2, 1
i+2, m−1
i+2, 0
Δi
L R
Δ ⊕ 0
Δ ⊕ 1
Δ ⊕ 2
Δ ⊕ 3
Δ ⊕ 4
Δ ⊕ 5
Δ ⊕ 6
Δ ⊕ 7
0, 6
L* R*

Previous results on AEZ

- AEZv3: birthday attack recovers the key [Asiacrypt 2015]
- Patched in AEZv4
  - Using Blake2 for key derivation
  - Bigger is better?
- AEZv4: birthday attack recovers the key [FSE 2017]

Previous results on AEZ

- AEZv3: birthday attack recovers the key [Asiacrypt 2015]
- Patched in AEZv4
  - Using Blake2 for key derivation
  - Bigger is better?
- AEZv4: birthday attack recovers the key [FSE 2017]

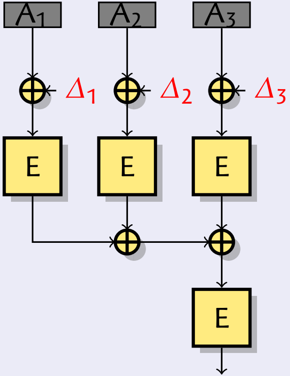
Previous results on AEZ

- AEZv3: birthday attack recovers the key [Asiacrypt 2015]
- Patched in AEZv4
  - Using Blake2 for key derivation
  - Bigger is better?
- AEZv4: birthday attack recovers the key [FSE 2017]

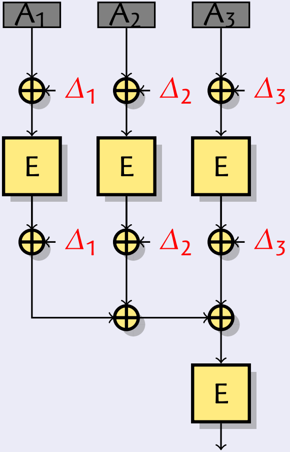
AEZ-MAC (PMAC variant)

- With empty message, AEZ turns into a MAC

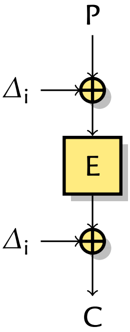
AEZv3



AEZv4



XEX construction



- $E(P \oplus \Delta_i) \oplus \Delta_i$ is a tweakable block cipher
  If $i \mapsto \Delta_i$ is an ε-AXU function
- Common constructions ($L = E_k(0)$)
  - $\Delta_i = i \cdot L$ (OCB1, OCB3)
  - $\Delta_i = 2^i \cdot L$ (OCB2)
- AEZv3 (subkeys J, L)
  - $\Delta_i = 8 \cdot J \oplus (i \bmod 8) \cdot J \oplus 2^{\lfloor (i-1)/8 \rfloor} \cdot L$
- AEZv4 (subkeys J, L)
  - $\Delta_i = L \oplus \left(2^{3+\lfloor (i-1)/8 \rfloor} + (i - 1 \bmod 8)\right) \cdot J$

A closer look

AEZv4 offsets

$$\Delta_i = L \oplus \left(2^{3+\lfloor (i-1)/8 \rfloor} + (i-1 \bmod 8)\right) \cdot J$$

- Addition between $GF(2^{128})$ elements?
- $\Delta_i = L \oplus 2^{3+\lfloor (i-1)/8 \rfloor} \cdot J \oplus (i-1 \bmod 8) \cdot J$
  - 2^x is actually α^x, with α a generator ($\alpha^{128} = \alpha^7 \oplus \alpha^2 \oplus \alpha \oplus 1$)
  - $(i-1 \bmod 8)$ is one of $\{0, 1, \alpha, \alpha \oplus 1, \alpha^2, \alpha^2 \oplus 1, \alpha^2 \oplus \alpha, \alpha^2 \oplus \alpha \oplus 1\}$
- Is it injective?
  - No!
  - $\Delta_{40} = L \oplus \alpha^7 \cdot J \oplus (\alpha^2 \oplus \alpha \oplus 1) \cdot J$
  - $\Delta_{1001} = L \oplus \alpha^{128} \cdot J = L \oplus (\alpha^7 \oplus \alpha^2 \oplus \alpha \oplus 1) \cdot J$

A closer look

AEZv4 offsets

$$\Delta_i = L \oplus \left(2^{3+\lfloor (i-1)/8 \rfloor} + (i-1 \bmod 8)\right) \cdot J$$

- Addition between $GF(2^{128})$ elements?
- $\Delta_i = L \oplus 2^{3+\lfloor (i-1)/8 \rfloor} \cdot J \oplus (i-1 \bmod 8) \cdot J$
  - 2^x is actually α^x, with α a generator ($\alpha^{128} = \alpha^7 \oplus \alpha^2 \oplus \alpha \oplus 1$)
  - $(i-1 \bmod 8)$ is one of $\{0, 1, \alpha, \alpha \oplus 1, \alpha^2, \alpha^2 \oplus 1, \alpha^2 \oplus \alpha, \alpha^2 \oplus \alpha \oplus 1\}$
- Is it injective?
  - No!
  - $\Delta_{40} = L \oplus \alpha^7 \cdot J \oplus (\alpha^2 \oplus \alpha \oplus 1) \cdot J$
  - $\Delta_{1001} = L \oplus \alpha^{128} \cdot J = L \oplus (\alpha^7 \oplus \alpha^2 \oplus \alpha \oplus 1) \cdot J$

A closer look

AEZv4 offsets

$$\Delta_i = L \oplus \left(2^{3+\lfloor(i-1)/8\rfloor} + (i-1 \bmod 8)\right) \cdot J$$

- Addition between GF(2^{128}) elements?
- $\Delta_i = L \oplus 2^{3+\lfloor(i-1)/8\rfloor} \cdot J \oplus (i-1 \bmod 8) \cdot J$
  - 2^x is actually α^x, with α a generator ($\alpha^{128} = \alpha^7 \oplus \alpha^2 \oplus \alpha \oplus 1$)
  - $(i-1 \bmod 8)$ is one of $\{0, 1, \alpha, \alpha \oplus 1, \alpha^2, \alpha^2 \oplus 1, \alpha^2 \oplus \alpha, \alpha^2 \oplus \alpha \oplus 1\}$
- Is it injective?
  - No!
  - $\Delta_{40} = L \oplus \alpha^7 \cdot J \oplus (\alpha^2 \oplus \alpha \oplus 1) \cdot J$
  - $\Delta_{1001} = L \oplus \alpha^{128} \cdot J = L \oplus (\alpha^7 \oplus \alpha^2 \oplus \alpha \oplus 1) \cdot J$

Conclusion

Forgery attack

- Swap A_{40} and A_{1001} $\leadsto$ same tag
- Swap $P_{79,80}$ and $P_{2001,2002}$ $\leadsto$ $C_{79,80}$ and $C_{2001,2002}$ swapped

- Similar to OTR attack
- Easy to patch: AEZv5?

- Even provably secure ciphers can be broken!

- Don't use AEZv4 to secure your toilet!