Building a Privacy-Preserving Smart Camera System

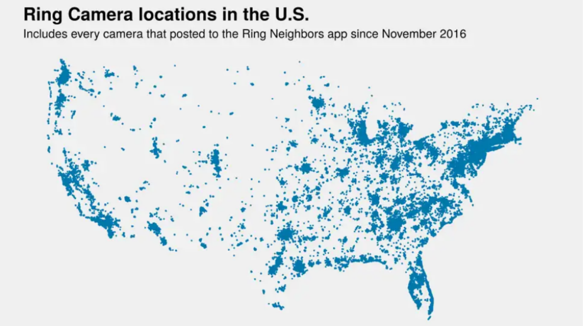
PennState

Systems and Internet Infrastructure Security Laboratory

Yohan Beugin, Quinn Burke, Blaine Hoak, Ryan Sheatsley, Eric Pauley,
Gang Tan, Syed Rafiul Hussain, Patrick McDaniel

PETS - July 11-15, 2022

Motivation



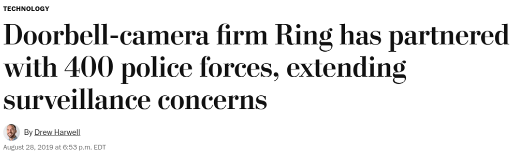
Ring Camera locations in the U.S.

Includes every camera that posted to the Ring Neighbors app since November 2016

Map from *Ring's Hidden Data Let Us Map Amazon's Sprawling Home Surveillance Network. Gizmodo, (2019)*.

Motivation

Obscure providers’ incentives

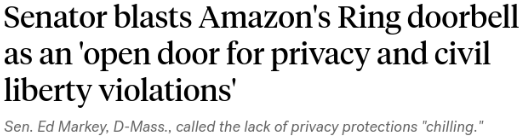


TECHNOLOGY

Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns

By Drew Harwell

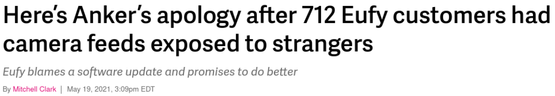
August 28, 2019 at 6:53 p.m. EDT



Senator blasts Amazon's Ring doorbell as an 'open door for privacy and civil liberty violations'

Sen. Ed Markey, D-Mass., called the lack of privacy protections "chilling."

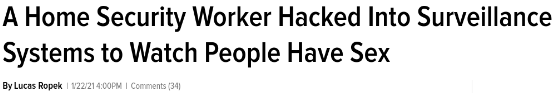
Untrustworthy providers



Here’s Anker’s apology after 712 Eufy customers had camera feeds exposed to strangers

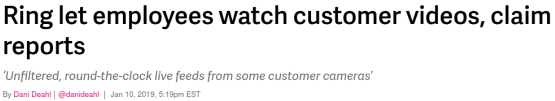
Eufy blames a software update and promises to do better

By Mitchell Clark | May 19, 2021, 3:09pm EDT



A Home Security Worker Hacked Into Surveillance Systems to Watch People Have Sex

By Lucas Ropek | 1/22/21 4:00PM | Comments (34)



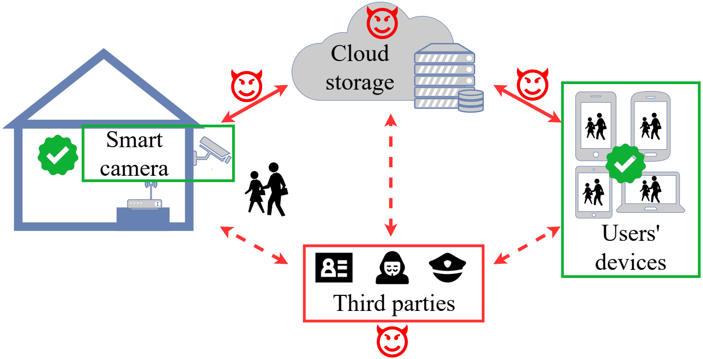
Ring let employees watch customer videos, claim reports

‘Unfiltered, round-the-clock live feeds from some customer cameras’

By Dani Deahl | @danideahl | Jan 10, 2019, 5:19pm EST

Goals

Smart camera systems need not compromise users privacy.



Goals

Smart camera systems need not compromise users privacy.

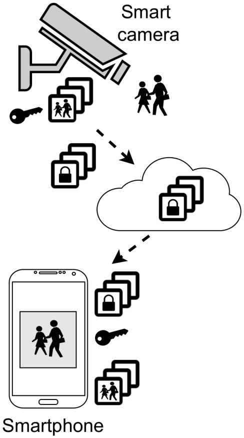
Return control to users

Support commercial features

Goals

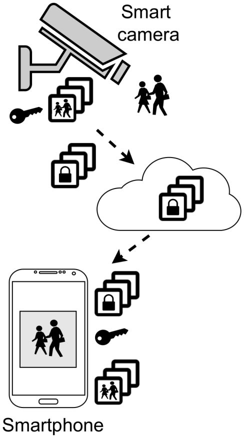
Return control to users

Support commercial features



Goals

Return control to users



Support commercial features

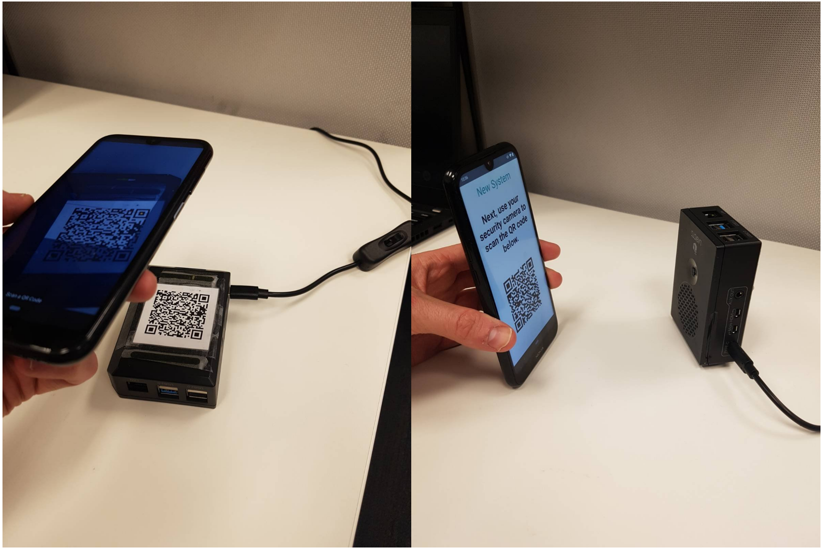
How to:

1. Establish root of trust?
2. Manage the keys?

Features:

- Configuration
- Recording and Streaming
- Delegation
- Deletion
- Recovery
- Reset

Establishing Root of Trust



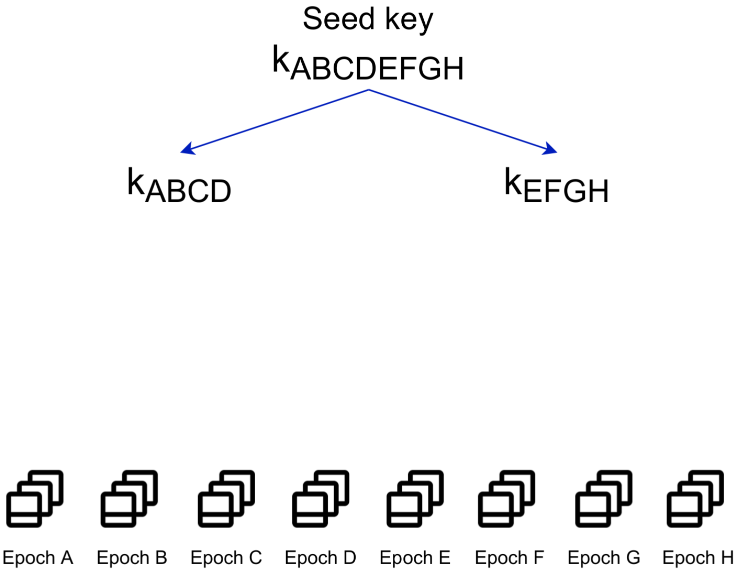
Key Management

Seed key

$k_{ABCDEFGH}$

Epoch A Epoch B Epoch C Epoch D Epoch E Epoch F Epoch G Epoch H

Key Management



Seed key

$k_{ABCDEFGH}$

k_{ABCD}

k_{EFGH}

Epoch A

Epoch B

Epoch C

Epoch D

Epoch E

Epoch F

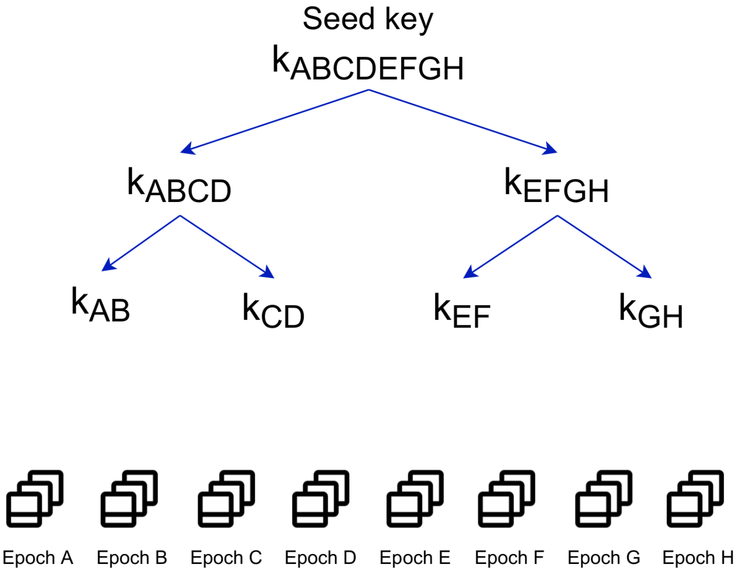
Epoch G

Epoch H

$$k_{left} = HKDF(k_{parent})$$

$$k_{right} = HKDF(k_{parent} \oplus 1)$$

Key Management



Seed key

$k_{ABCDEFGH}$

k_{ABCD}

k_{EFGH}

k_{AB}

k_{CD}

k_{EF}

k_{GH}

Epoch A

Epoch B

Epoch C

Epoch D

Epoch E

Epoch F

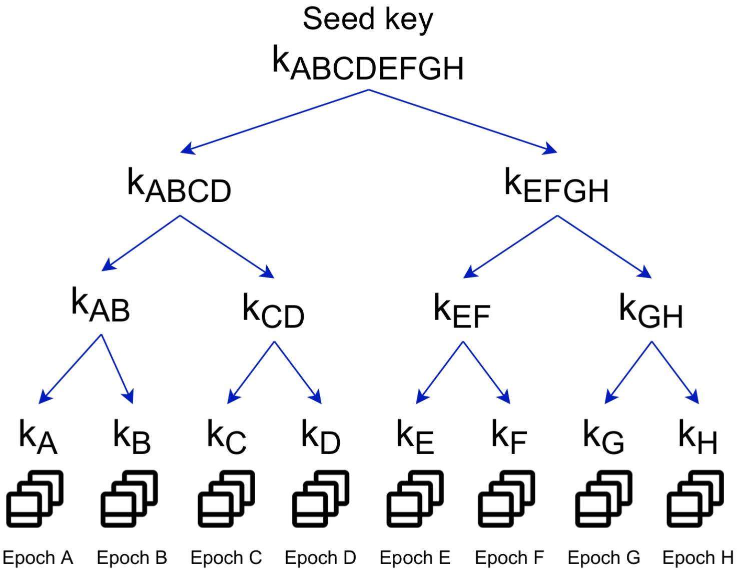
Epoch G

Epoch H

$$k_{left} = HKDF(k_{parent})$$

$$k_{right} = HKDF(k_{parent} \oplus 1)$$

Key Management



Seed key

$k_{ABCDEFGH}$

k_{ABCD} k_{EFGH}

k_{AB} k_{CD} k_{EF} k_{GH}

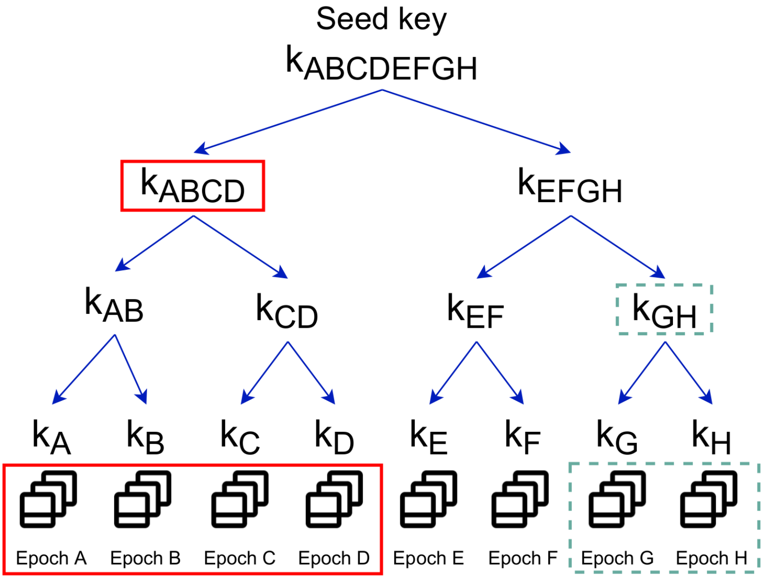
k_A k_B k_C k_D k_E k_F k_G k_H

Epoch A Epoch B Epoch C Epoch D Epoch E Epoch F Epoch G Epoch H

$$k_{left} = HKDF(k_{parent})$$

$$k_{right} = HKDF(k_{parent} \oplus 1)$$

Key Management

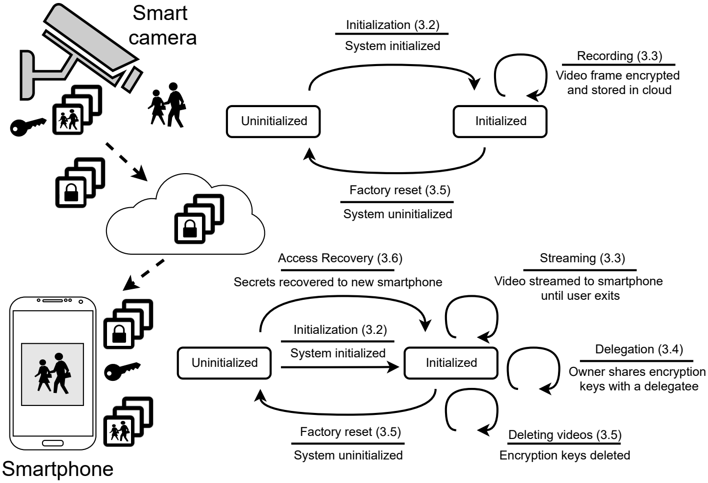


$$k_{left} = HKDF(k_{parent})$$

$$k_{right} = HKDF(k_{parent} \oplus 1)$$

☞ Fine-grained delegation

Camera system Controlled Totally by Users



Evaluation

Privacy and security analysis:

1. Right to not be seen
2. Right of sole ownership
3. Right to be forgotten

Evaluation

Privacy and security analysis:

1. Right to not be seen
2. Right of sole ownership
3. Right to be forgotten

Performance evaluation

Device	Operation	Delay	σ
Camera	Key Extraction	0.05 ms	0.2 ms
	Frame Encryption	4.0 ms	1.3 ms
	Signature	8.8 ms	2.8 ms
	Upload	662 ms	536 ms
Smartphone	Download	204 ms	358 ms
	Signature Verification	0.7 ms	0.5 ms
	Key Extraction	0.03 ms	0.3 ms
	Frame Decryption	0.6 ms	0.6 ms

Table: Average delay during live stream at 480 p (1000 frames)

Evaluation

Privacy and security analysis:

1. Right to not be seen
2. Right of sole ownership
3. Right to be forgotten

Performance evaluation

Device	Operation	Delay	σ
Camera	Key Extraction	$0.05\,\mathrm{ms}$	$0.2\,\mathrm{ms}$
	Frame Encryption	$4.0\,\mathrm{ms}$	$1.3\,\mathrm{ms}$
	Signature	$8.8\,\mathrm{ms}$	$2.8\,\mathrm{ms}$
	Upload	$662\,\mathrm{ms}$	$536\,\mathrm{ms}$
Smartphone	Download	$204\,\mathrm{ms}$	$358\,\mathrm{ms}$
	Signature Verification	$0.7\,\mathrm{ms}$	$0.5\,\mathrm{ms}$
	Key Extraction	$0.03\,\mathrm{ms}$	$0.3\,\mathrm{ms}$
	Frame Decryption	$0.6\,\mathrm{ms}$	$0.6\,\mathrm{ms}$

Table: Average delay during live stream at $480\,\mathrm{p}$ (1000 frames)

Functional user evaluation

- ☞ Usable and simple
- ☞ Fine-grained delegation
- ☞ Sufficient quality
- ☞ Improvements: latency and motion detection

Conclusion

No need to compromise users privacy:

1. Return full control to users:
   - Root of trust
   - Complete mediation
2. Support commercial functionality
3. Extensible to other IoT devices

Paper: *Building a Privacy-Preserving Smart Camera System*

Code: https://github.com/siis/CaCTUs

✉ yohan@beugin.org 🏠 https://yohan.beugin.org