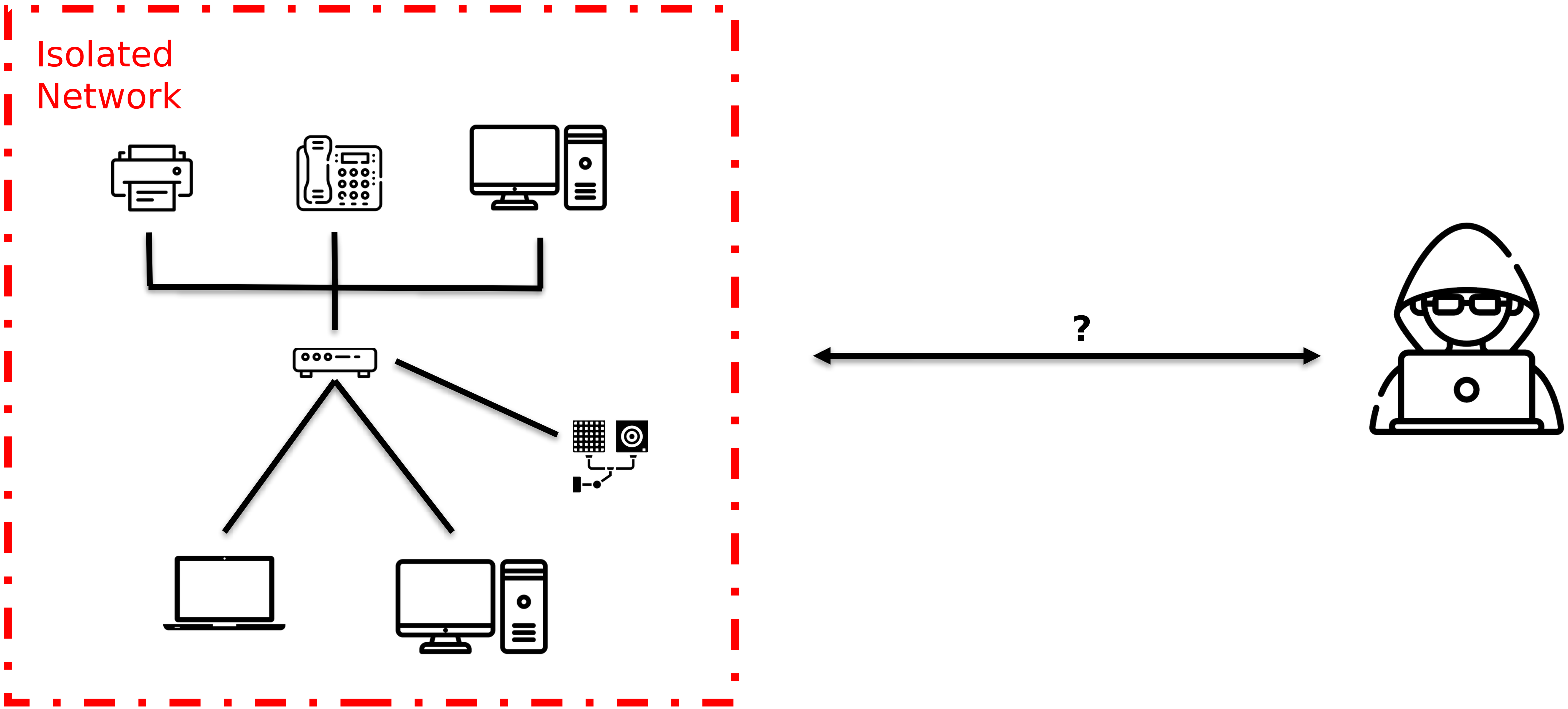
LaserShark 🦈

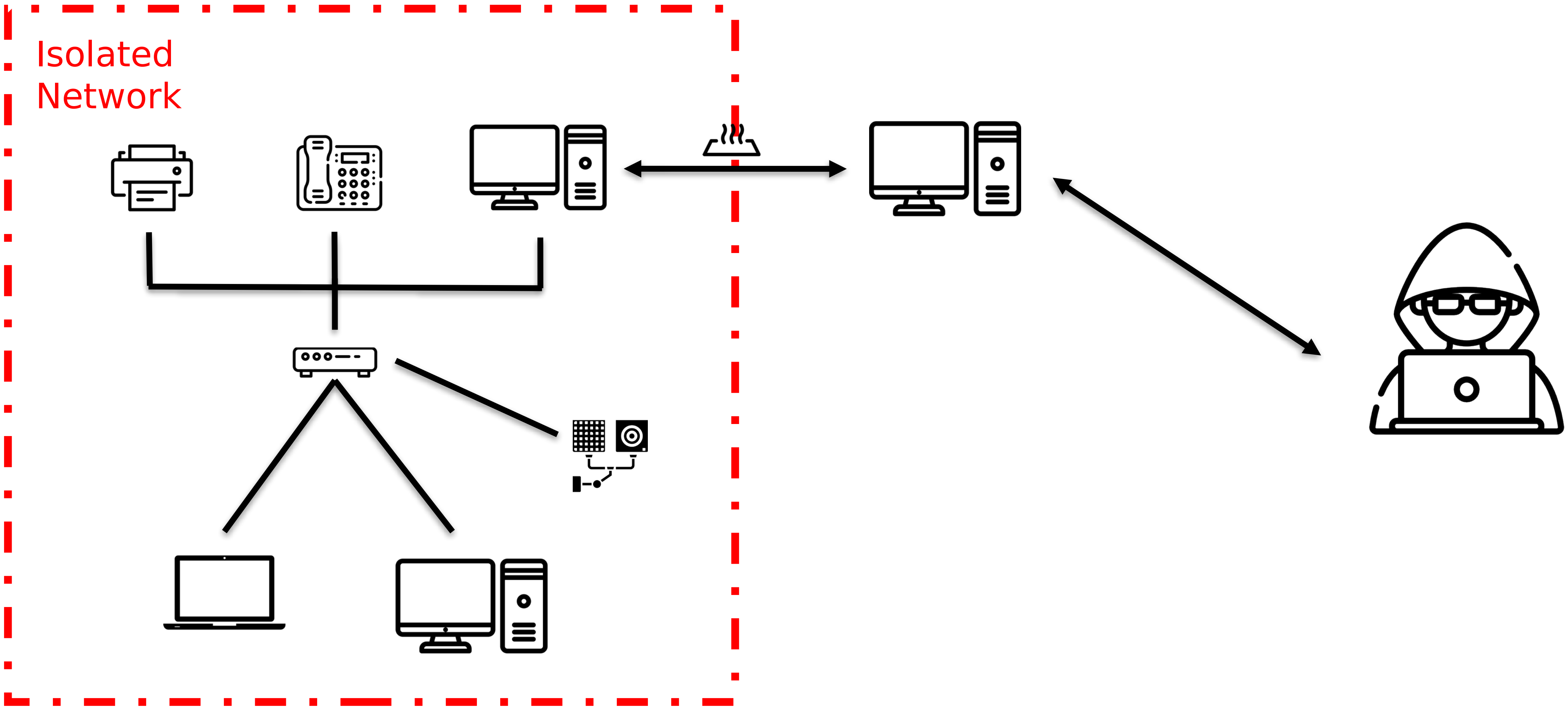
Establishing Fast, Bidirectional Communication into Air-Gapped Systems

Niclas Kühnapfel, Stefan Preußler, Maximilian Noppel, Thomas Schneider, Konrad Rieck, Christian Wressnegger

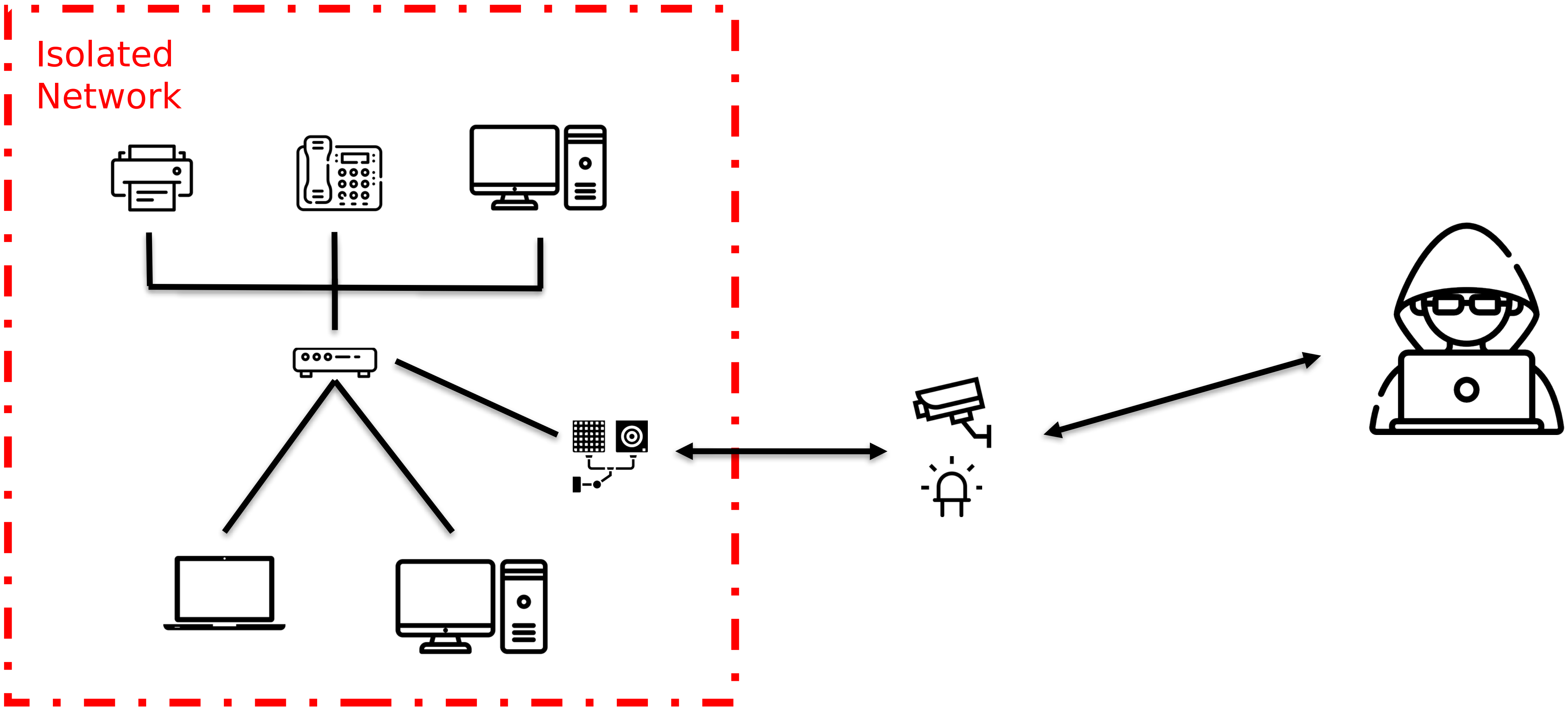
Bridging the Air Gap



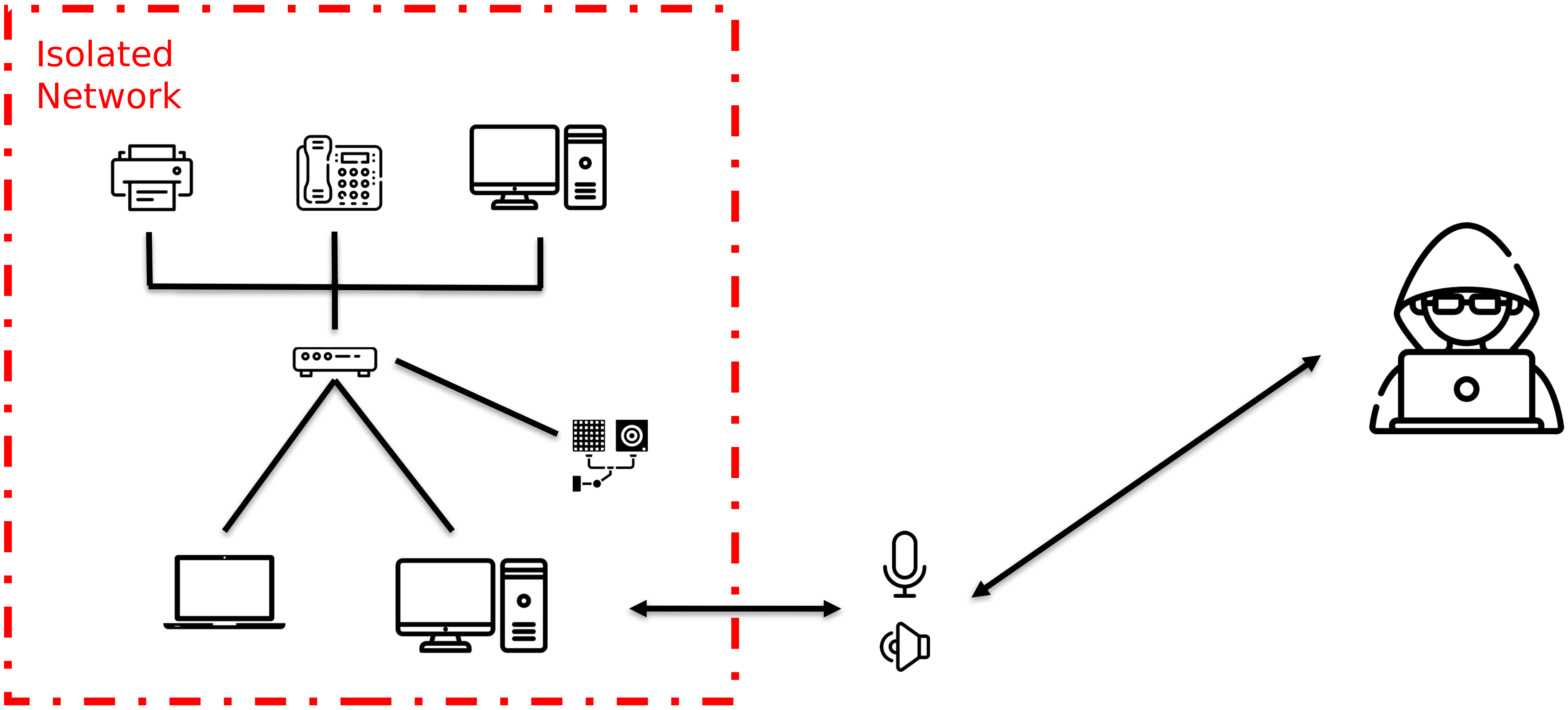
Bridging the Air Gap



Bridging the Air Gap

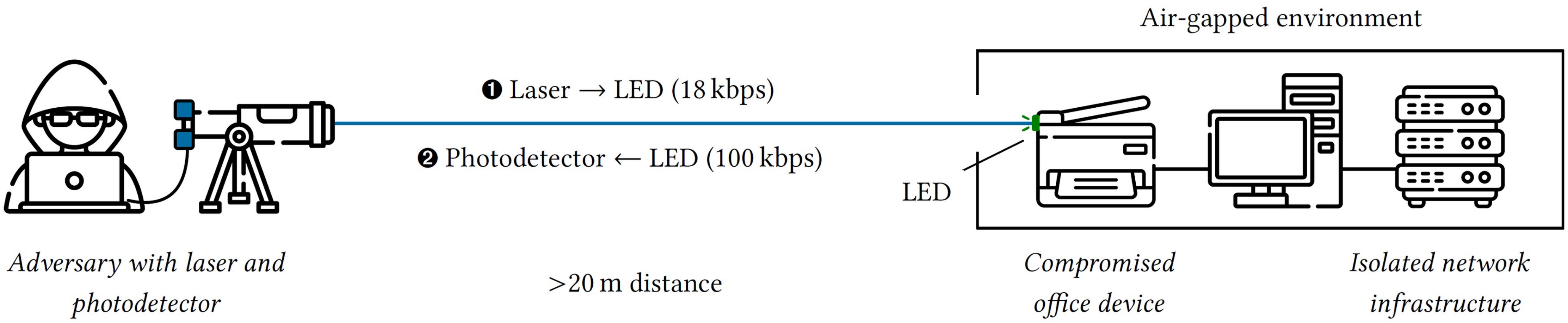


Bridging the Air Gap

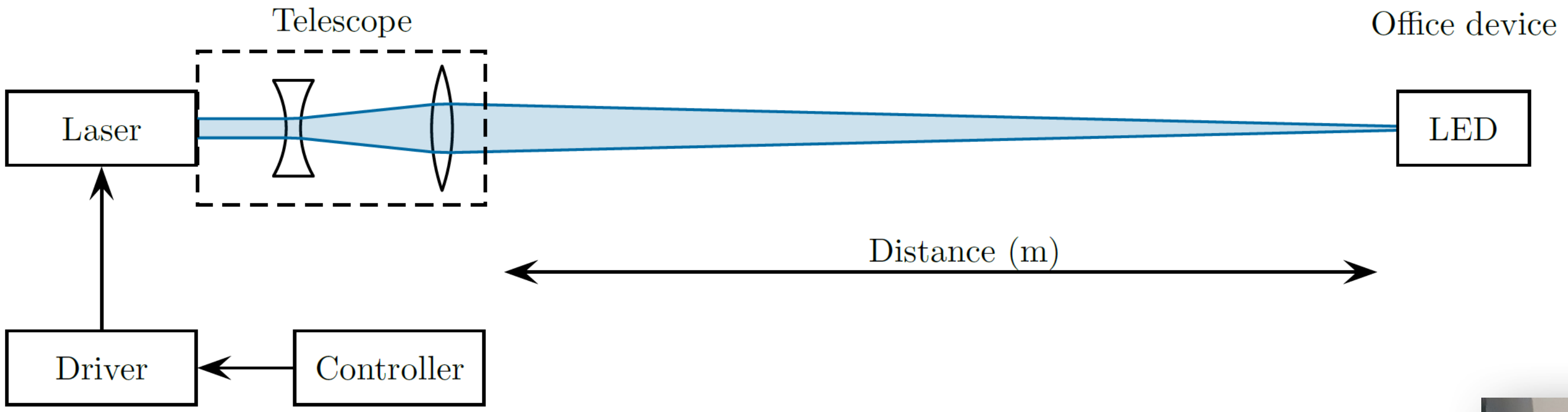


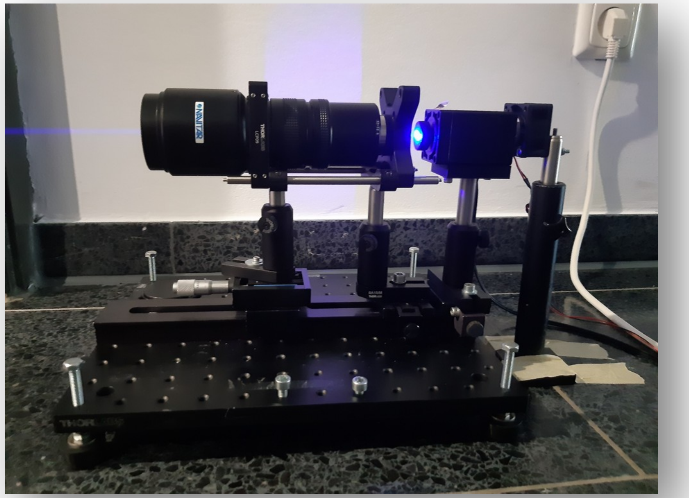
Our Approach

- Novel infiltration technique
- Significantly faster
- Practical implementation

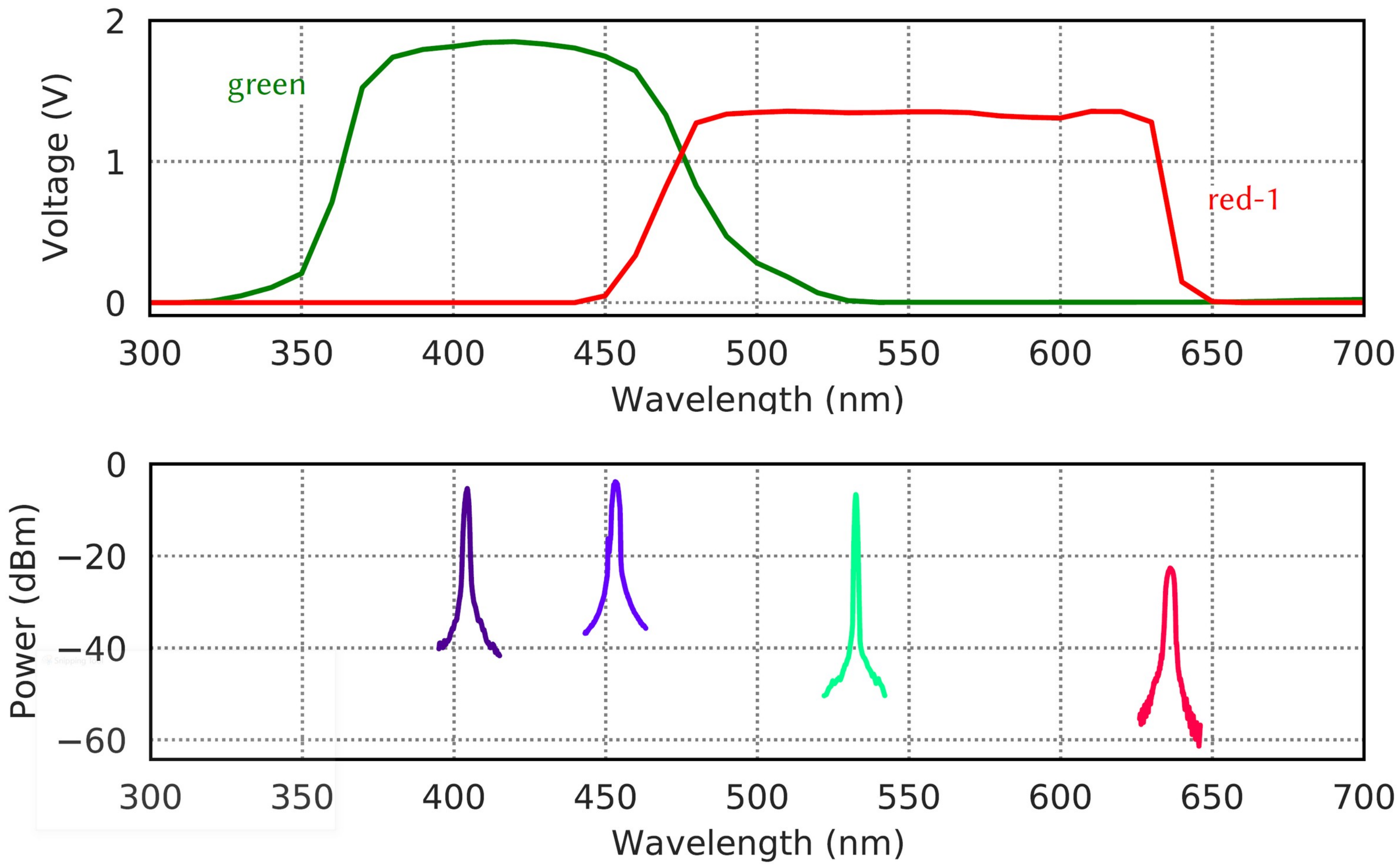


Infiltrating Data

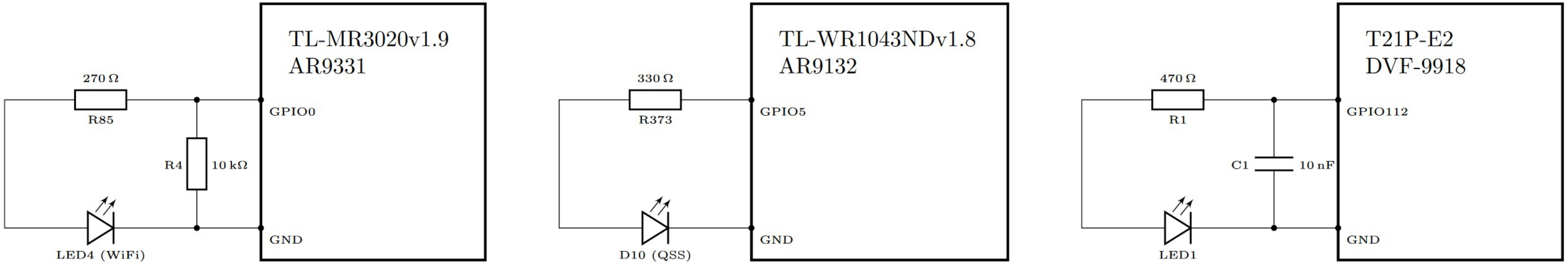




Laser and LED Spectra



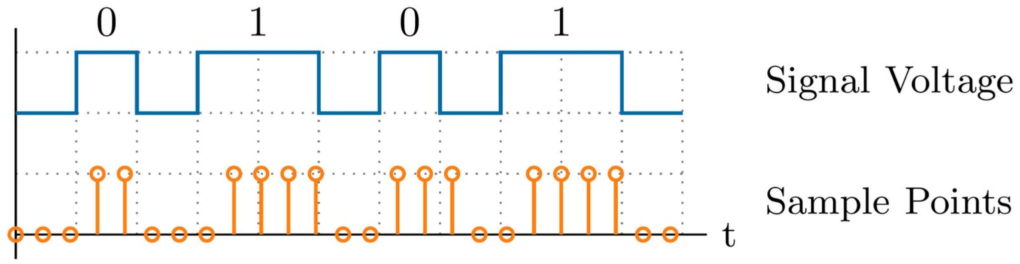
Targets


TL-MR3020v1.9
AR9331
270 Ω
R85
R4
10 kΩ
GPIO0
GND
LED4 (WiFi)
TL-WR1043NDv1.8
AR9132
330 Ω
R373
GPIO5
GND
D10 (QSS)
T21P-E2
DVF-9918
470 Ω
R1
C1
10 nF
GPIO112
GND
LED1

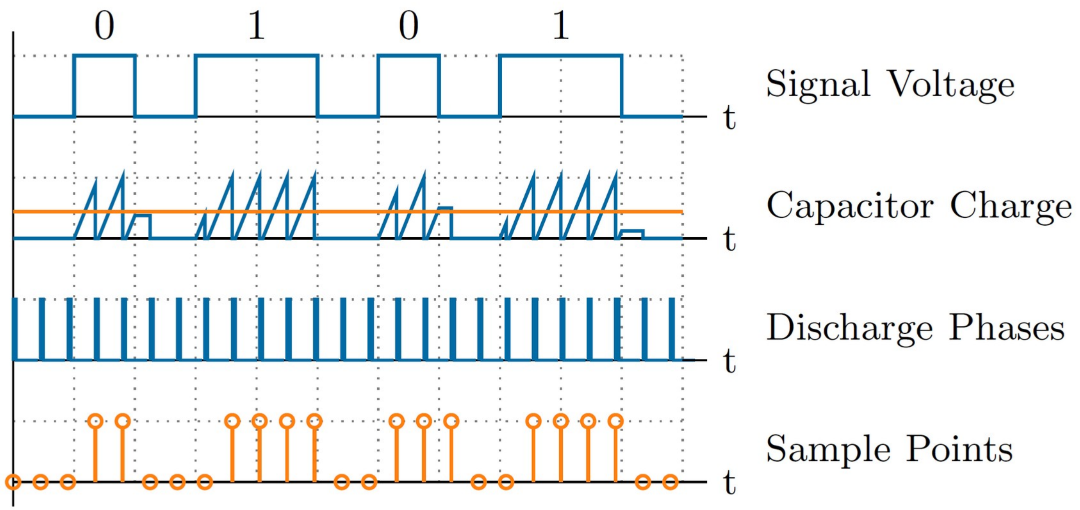
(a) (b) (c)

Modulation & Sampling

- Robust and easy modulation
- Like PWM or morse code
- Immediate sampling
- Delayed sampling



Immediate
Sampling



Delayed
Sampling

Results

- Distance of 30 cm
- Empirical upper limit for each device

Target device	Processor		Laser	LED	GPIO	$t_{1\text{-bit}}$	$t_{0\text{-bit}}$	t_{off}	Data rate
TP-Link TL-MR3020	Atheros AR-9331	(400 MHz)	green	green	0 (WiFi LED)	200 µs	100 µs	100 µs	3,333 bps
TP-Link TL-WR1043ND	Atheros AR-9132	(400 MHz)	violet	green	5 (QSS LED)	150 µs	75 µs	100 µs	4,000 bps
Raspberry Pi	BCM2837B0	(1.4 GHz)	violet	green[b]	26 (Pin Header)	30 µs	15 µs	15 µs	22,222 bps
Yealink SIP-T21P E2	DSPG DVF-9918	(400 MHz)	violet	green	112 (green/red button)	700 µs	350 µs	300 µs	1,000 bps
Raspberry Pi (with 10 nF capacitor)	BCM2837B0	(1.4 GHz)	violet	green[b]	26 (Pin Header)	320 µs	180 µs	180 µs	2,000 bps

[b] Using the LEDs of the Yealink SIP-T21P E2 telephone.

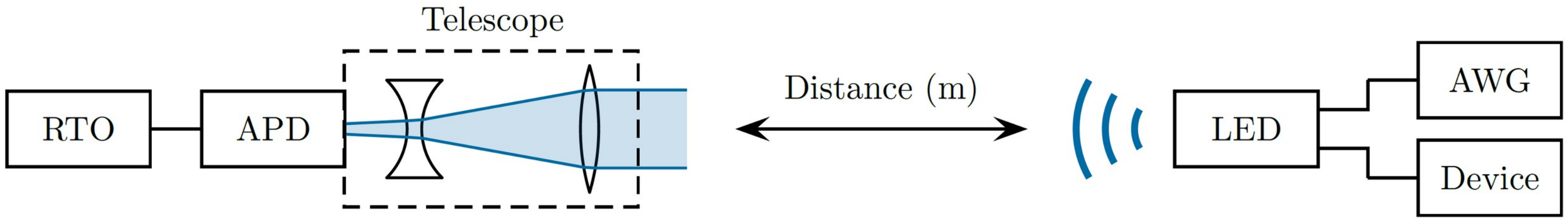
Results

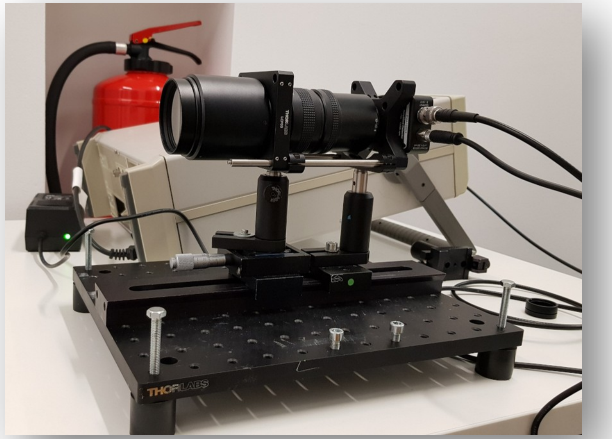
- Raspberry Pi with both circuit types
- MOSQUITO: 166 bps (3 m), 10 bps (9 m)

Distance	Target Circuit		Laser	At the Target		Configuration			Data rate
	Resistor	Capacitor	Input Current	Optical Power	Current	$t_{1\text{-bit}}$	$t_{0\text{-bit}}$	t_{off}	
10 m	●		1 A	12 mW	37 µA	40 µs	15 µs	15 µs	18.2 kbps
20 m	●		2 A	58 mW	43 µA	40 µs	15 µs	15 µs	18.2 kbps
25 m	●		2 A	37 mW	20 µA	40 µs	15 µs	15 µs	18.2 kbps
30 m	●		4 A	50 mW	32 µA	40 µs	15 µs	15 µs	18.2 kbps
35 m	●		4 A	45 mW	35 µA	50 µs	15 µs	25 µs	13.3 kbps
40 m	●		4 A	35 mW	20 µA	–	–	–	✗
35 m		●	4 A	45 mW	35 µA	3,800 µs	2,100 µs	1,200 µs	200 bps
40 m		●	4 A	35 mW	20 µA	3,800 µs	2,100 µs	1,200 µs	200 bps

Exfiltrating Data

- High-speed camera
- Avalanche photodiode





Results

- Raspberry Pi + IP phone‘s green LED
- LED-it-GO: 4,000 bps (8 m)

Distance	Data rate			
	1 kbps	50 kbps	100 kbps	200 kbps
5 m	0.0 %	0.0 %	0.0 %	0.1 %
10 m	0.0 %	0.0 %	0.0 %	0.9 %
15 m	0.0 %	0.0 %	0.0 %	2.2 %
20 m	0.0 %	0.0 %	0.1 %	✗
25 m	0.0 %	0.0 %	0.1 %	✗
30 m	✗	✗	✗	✗

APD as receiver

Target device	Distance	Data rate
TP-Link TL-MR3020	2 − 40 m	119.05 bps
TP-Link TL-WR1043ND	2 − 40 m	119.05 bps
Yealink SIP-T21P E2	2 − 40 m	119.05 bps

Camera as receiver

Summary

- Covert bidirectional communication channel
- Direct line of sight necessary
- No hardware modifications
- Infiltration of data at 18.2 kbps over 30m
- Exfiltration of data at 100 kbps over 25m

Thanks!

https://intellisec.de/research/lasershark

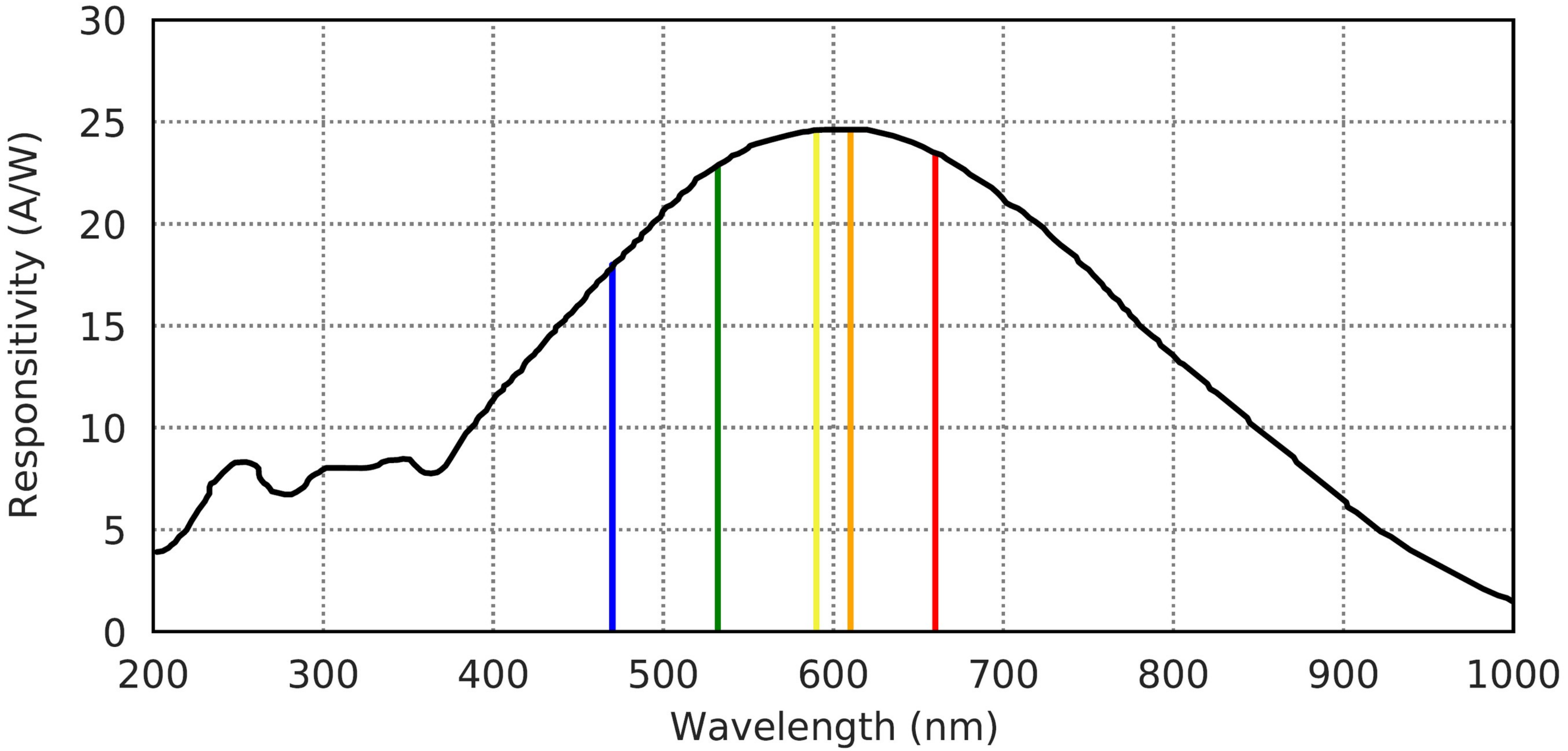
https://github.com/intellisec/lasershark

Karlsruher Institut für Technologie

Technische Universität Braunschweig

Niclas Kühnapfel, Stefan Preußler, Maximilian Noppel, Thomas Schneider, Konrad Rieck, Christian Wressnegger

Avalanche Photodiode Spectrum



Data rate for each Target

Target device	Processor		Laser	LED	GPIO	$t_{1\text{-bit}}$	$t_{0\text{-bit}}$	t_{off}	Data rate
TP-Link TL-MR3020	Atheros AR-9331	(400 MHz)	green	green	0 (WiFi LED)	200 µs	100 µs	100 µs	3,333 bps
TP-Link TL-WR1043ND	Atheros AR-9132	(400 MHz)	violet	green	5 (QSS LED)	150 µs	75 µs	100 µs	4,000 bps
Raspberry Pi	BCM2837B0	(1.4 GHz)	violet	green[b]	26 (Pin Header)	30 µs	15 µs	15 µs	22,222 bps
Yealink SIP-T21P E2	DSPG DVF-9918	(400 MHz)	violet	green	112 (green/red button)	700 µs	350 µs	300 µs	1,000 bps
Raspberry Pi (with 10 nF capacitor)	BCM2837B0	(1.4 GHz)	violet	green[b]	26 (Pin Header)	320 µs	180 µs	180 µs	2,000 bps

[b] Using the LEDs of the Yealink SIP-T21P E2 telephone.