black hat®
USA 2017

JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

Daniele Lain
University of Padua

Prof. Mauro Conti - *Univ. of Padua*
Prof. Gene Tsudik - *UC Irvine*
Dr. Alberto Compagno - *Sapienza Univ. of Rome*

SKYPE & TYPE

Keystroke Leakage over VoIP

Meet our monkey.

Meet our monkey.

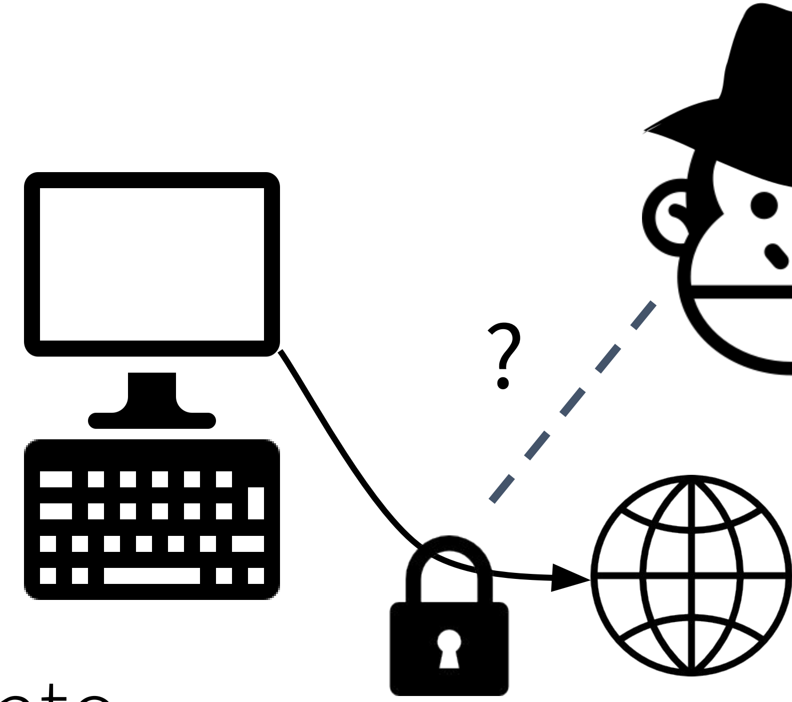
Our monkey is a scoundrel.

Meet our monkey.

Our monkey is a scoundrel.

Monkey likes secrets, but is very bad at crypto.

(just like me)

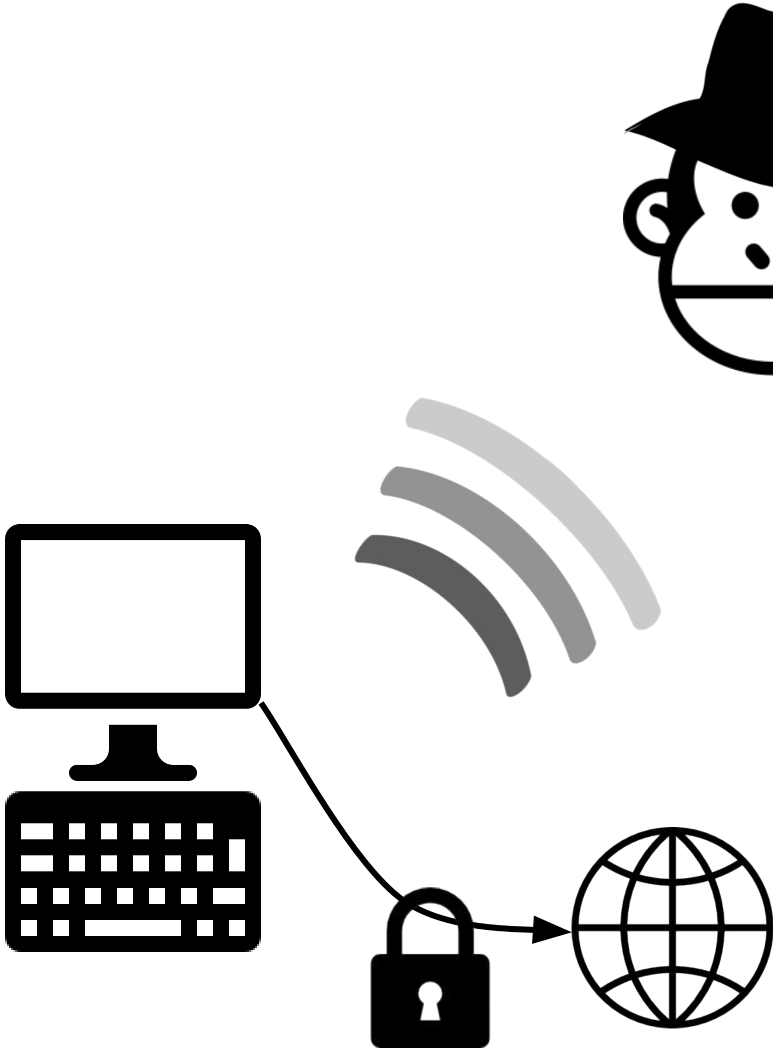


But monkeys have **very** good hearing

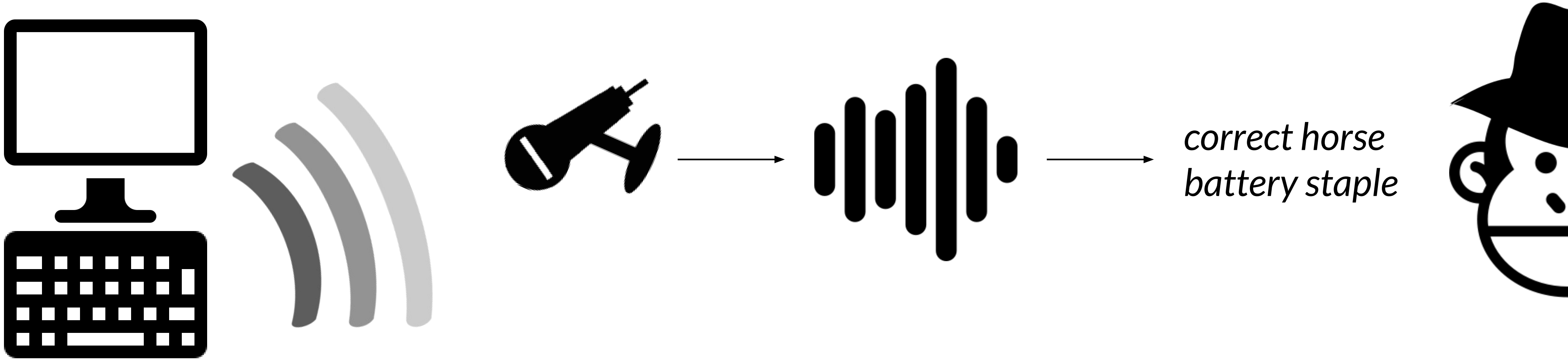
(unlike me)

And keyboard keys have unique sounds

So let's listen!



Keyboard Acoustic Eavesdropping



correct horse battery staple

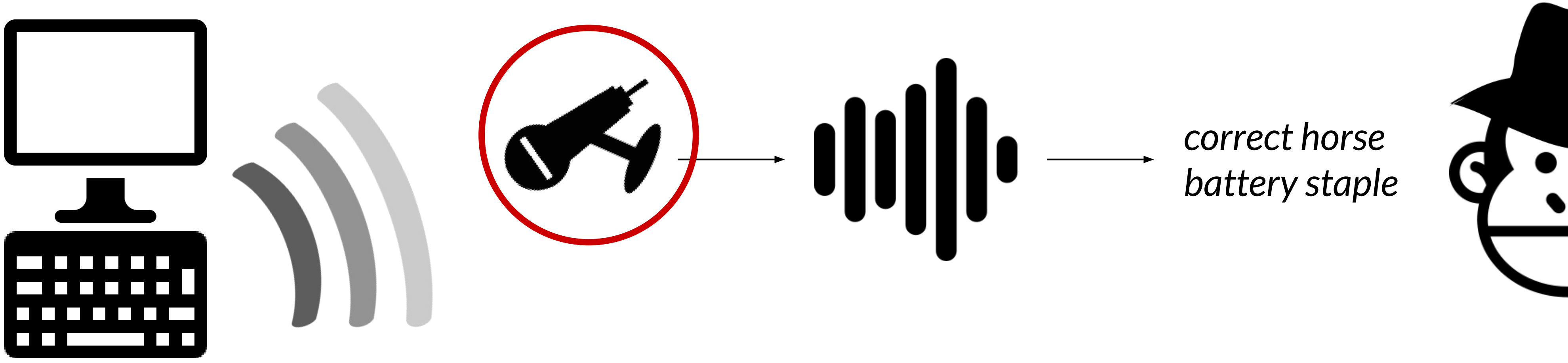
Supervised Learning **(Asonov, 2004; Halevi, 2012; 2014)**

- *Less input assumptions*

Unsupervised Learning **(Berger, 2006; Zhuang, 2009)**

- *More general*

Keyboard Acoustic Eavesdropping



Supervised Learning **(Asonov, 2004; Halevi, 2012; 2014)**

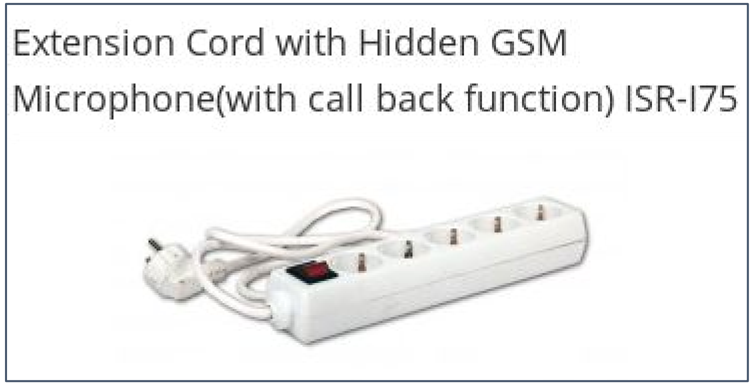
- *Less input assumptions*

Unsupervised Learning **(Berger, 2006; Zhuang, 2009)**

- *More general*

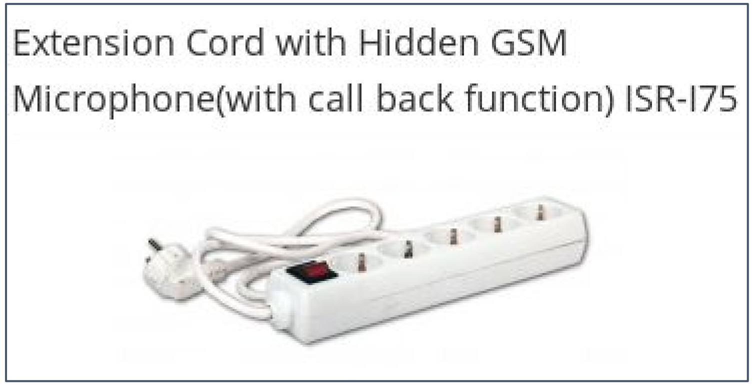
LET’S HACK

Spying Devices and How to Plant Them

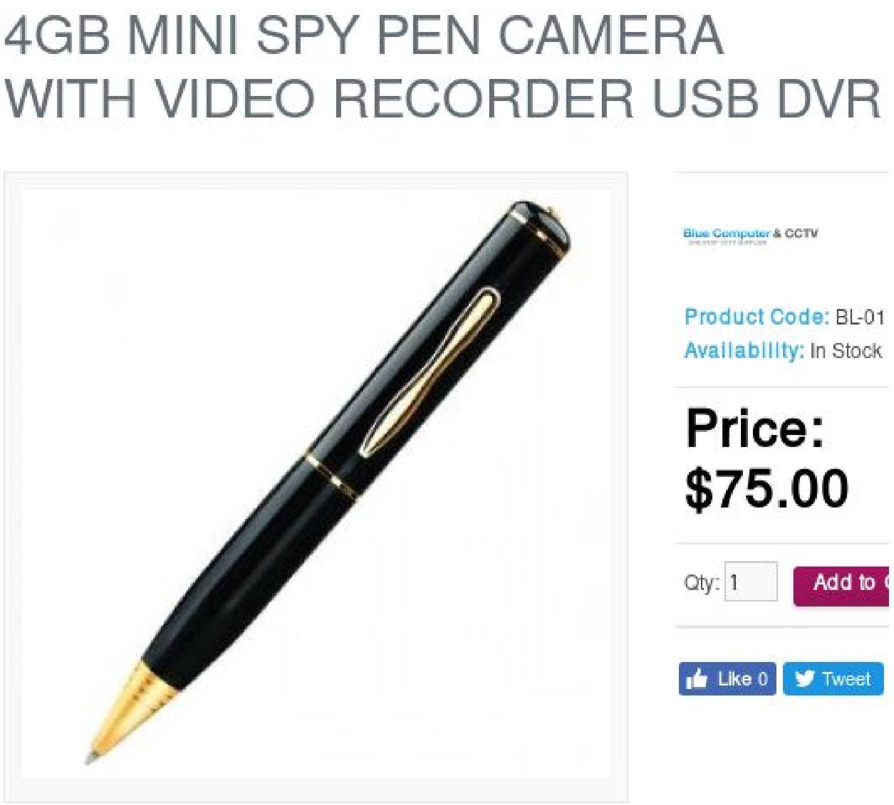


Extension Cord with Hidden GSM Microphone(with call back function) ISR-I75

Spying Devices and How to Plant Them



Extension Cord with Hidden GSM Microphone(with call back function) ISR-I75



4GB MINI SPY PEN CAMERA WITH VIDEO RECORDER USB DVR

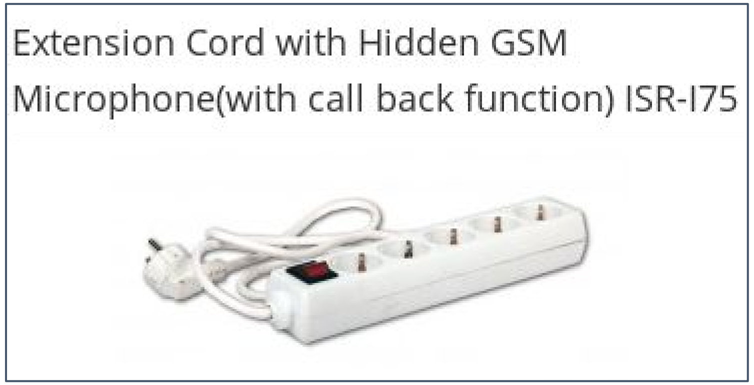
Product Code: BL-01

Availability: In Stock

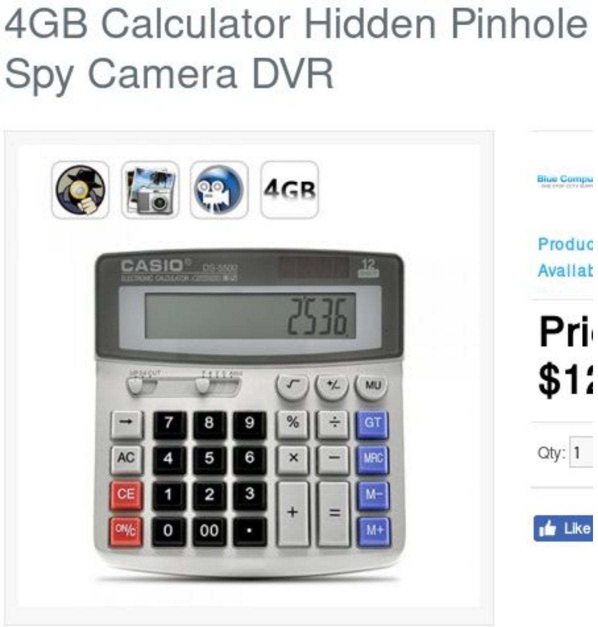
Price: $75.00

Qty: 1

Spying Devices and How to Plant Them



Extension Cord with Hidden GSM Microphone(with call back function) ISR-I75



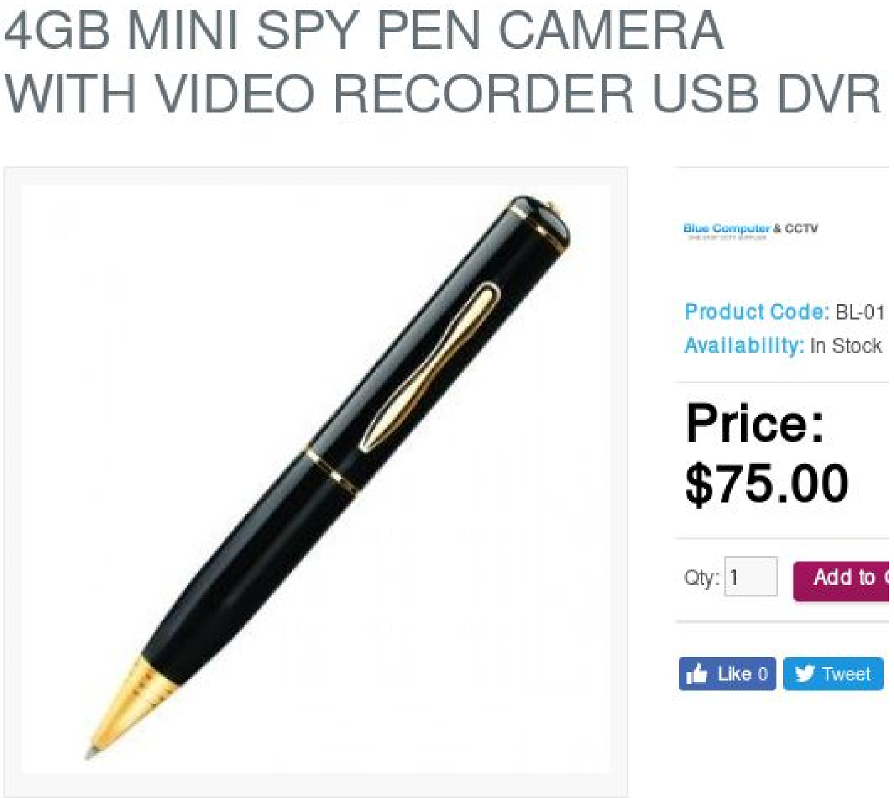
4GB Calculator Hidden Pinhole Spy Camera DVR

Blue Compu

Produc
Availat

Pri
$12

Qty: 1



4GB MINI SPY PEN CAMERA WITH VIDEO RECORDER USB DVR

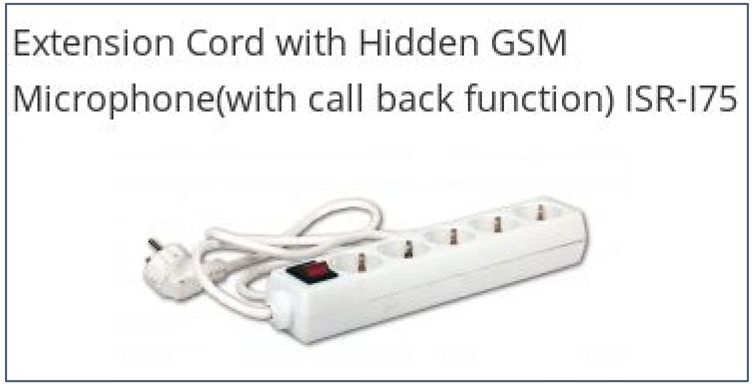
Blue Computer & CCTV

Product Code: BL-01
Availability: In Stock

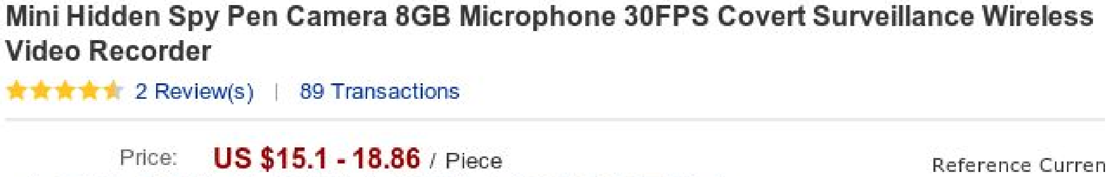
Price:
$75.00

Qty: 1

Spying Devices and How to Plant Them



Extension Cord with Hidden GSM Microphone(with call back function) ISR-I75

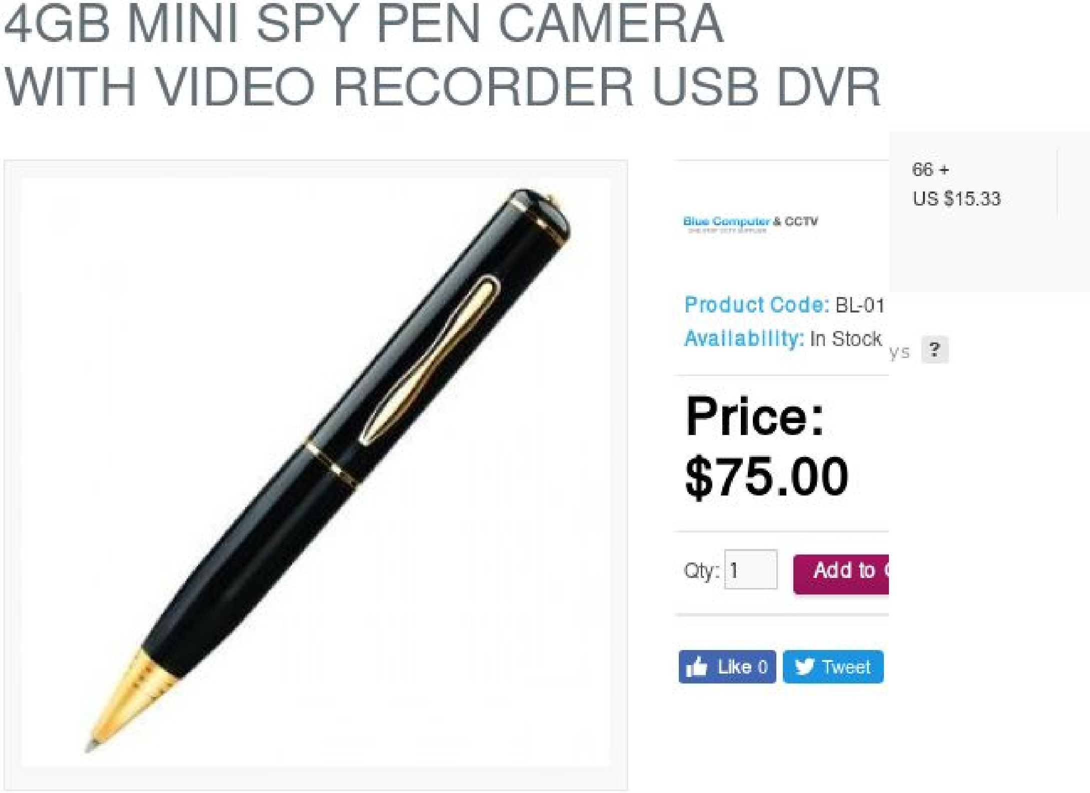


Mini Hidden Spy Pen Camera 8GB Microphone 30FPS Covert Surveillance Wireless Video Recorder

★★★★★ 2 Review(s) | 89 Transactions

Price: US $15.1 - 18.86 / Piece

Reference Curren



4GB MINI SPY PEN CAMERA WITH VIDEO RECORDER USB DVR

66 +
US $15.33

Blue Computer & CCTV

Product Code: BL-01

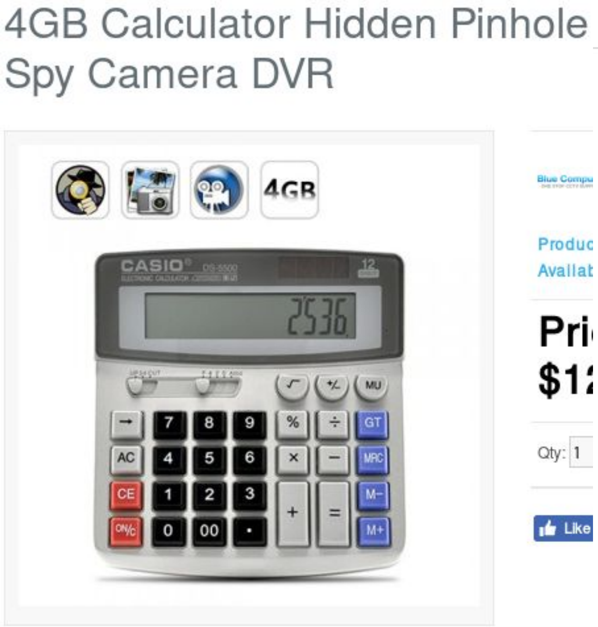
Availability: In Stock

ys ?

Price: $75.00

Qty: 1 Add to

Like 0 Tweet



4GB Calculator Hidden Pinhole Spy Camera DVR

Blue Compu

Produc

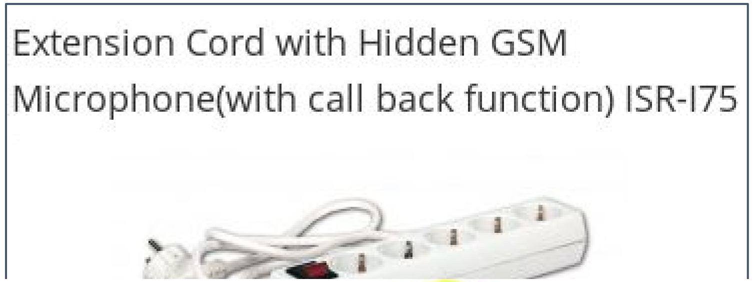
Availat

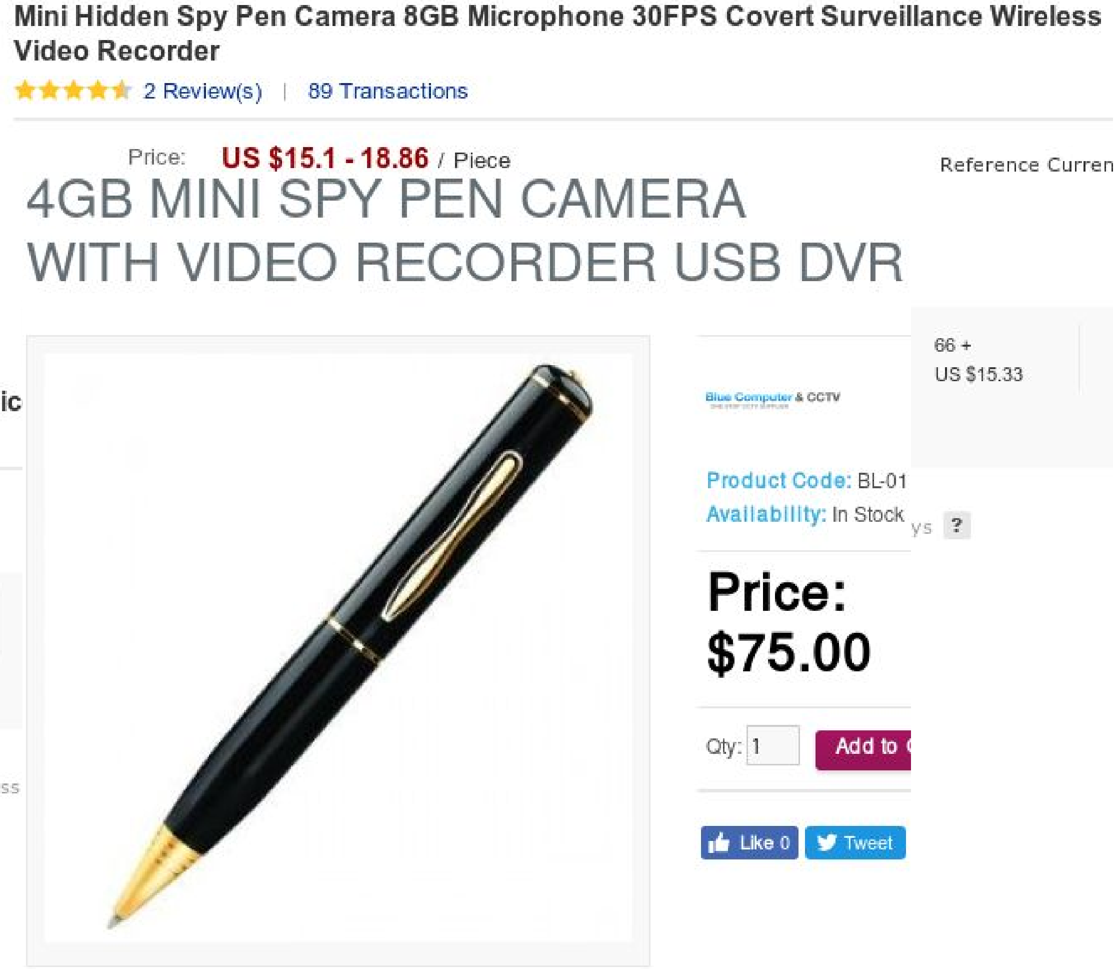
Pri
$12

Qty: 1

Like

Spying Devices and How to Plant Them


Extension Cord with Hidden GSM Microphone(with call back function) ISR-I75


Mini Hidden Spy Pen Camera 8GB Microphone 30FPS Covert Surveillance Wireless Video Recorder

★★★★★ 2 Review(s) | 89 Transactions

Price: US $15.1 - 18.86 / Piece

Reference Curren

4GB MINI SPY PEN CAMERA WITH VIDEO RECORDER USB DVR

66 +
US $15.33

Blue Computer & CCTV

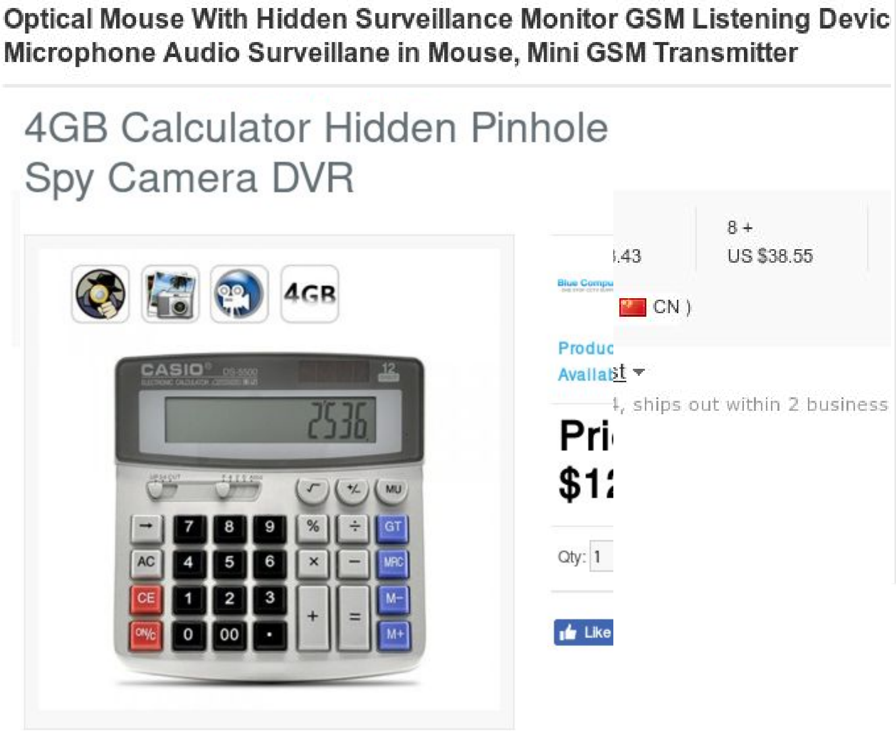
Product Code: BL-01
Availability: In Stock

ys ?

Price:
$75.00

Qty: 1 Add to (

Like 0 Tweet


Optical Mouse With Hidden Surveillance Monitor GSM Listening Devic Microphone Audio Surveillane in Mouse, Mini GSM Transmitter

4GB Calculator Hidden Pinhole Spy Camera DVR

.43

8 +
US $38.55

Blue Compu

CN)

Produc
Availast

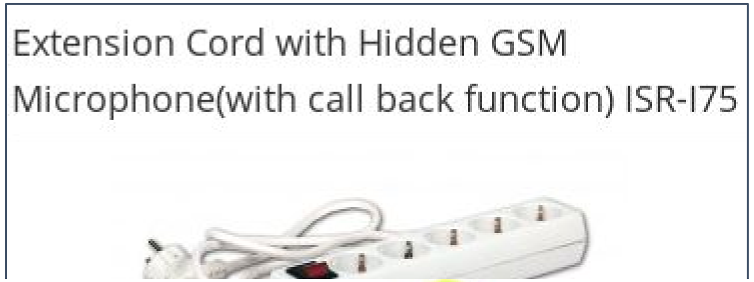
, ships out within 2 business

Pri
$1

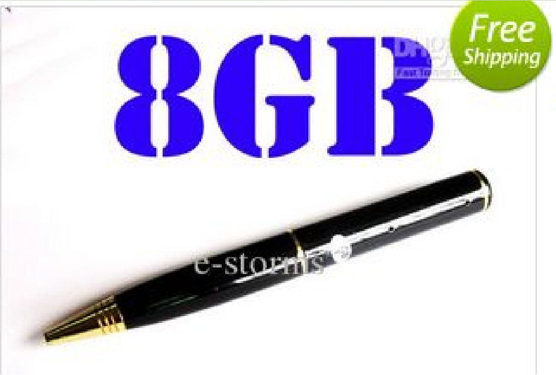
Qty: 1

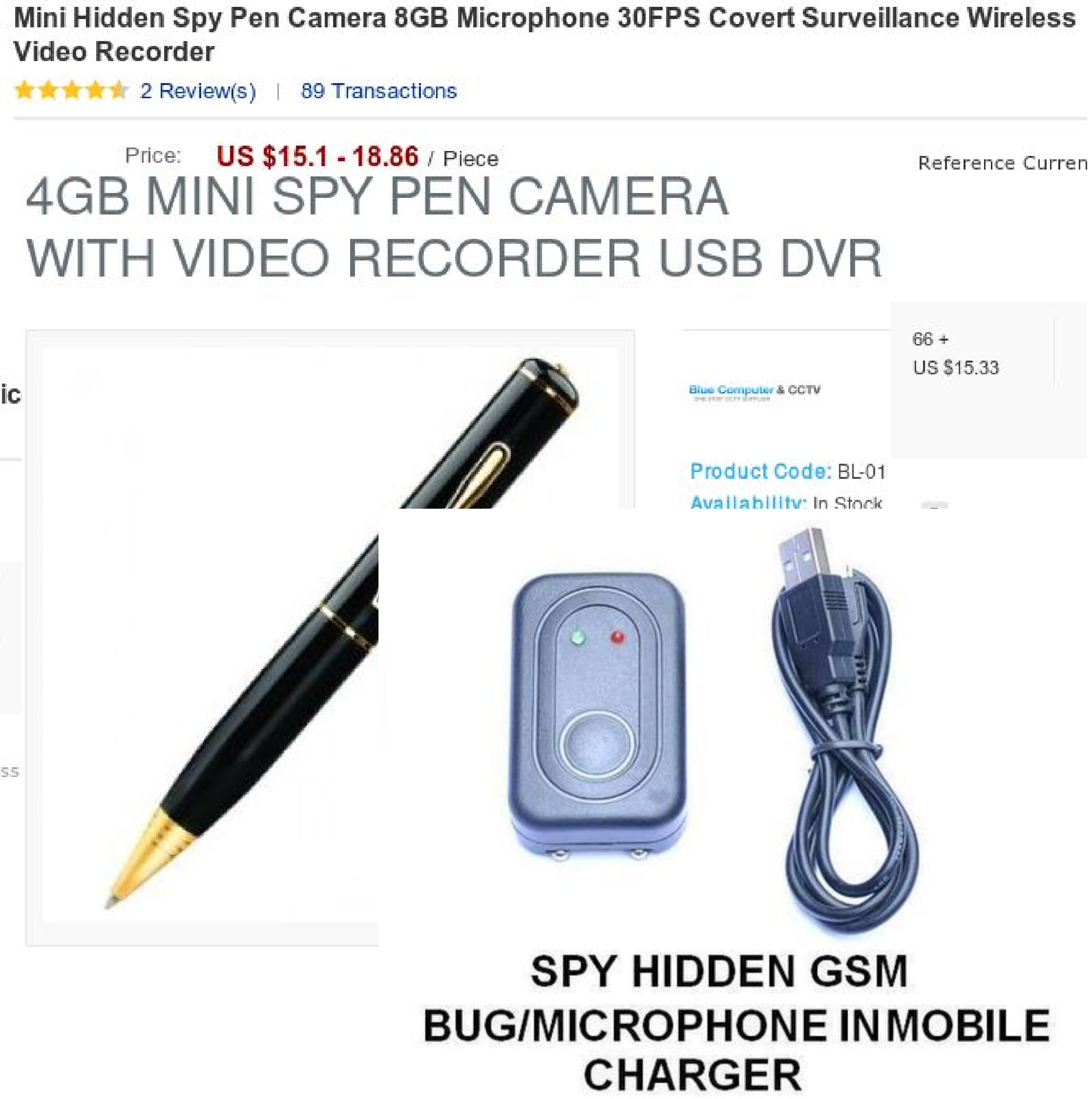
Like

Spying Devices and How to Plant Them



Extension Cord with Hidden GSM Microphone(with call back function) ISR-I75





Mini Hidden Spy Pen Camera 8GB Microphone 30FPS Covert Surveillance Wireless Video Recorder

★★★★★ 2 Review(s) | 89 Transactions

Price: US $15.1 - 18.86 / Piece

Reference Curren

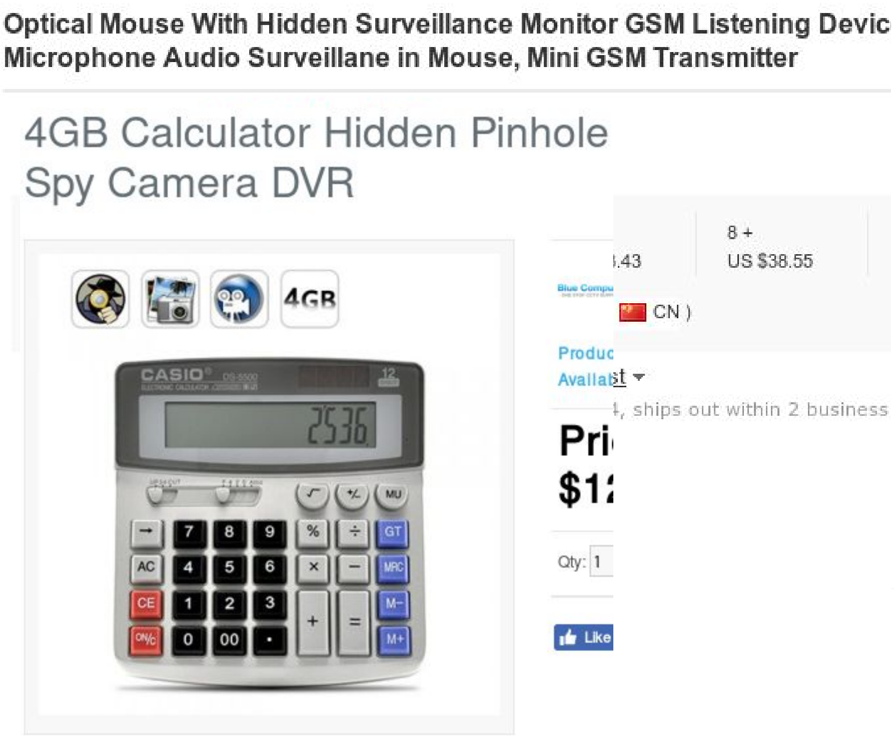
4GB MINI SPY PEN CAMERA WITH VIDEO RECORDER USB DVR

66 +
US $15.33

Blue Computer & CCTV

Product Code: BL-01
Availability: In Stock

SPY HIDDEN GSM BUG/MICROPHONE IN MOBILE CHARGER



Optical Mouse With Hidden Surveillance Monitor GSM Listening Devic
Microphone Audio Surveillane in Mouse, Mini GSM Transmitter

4GB Calculator Hidden Pinhole Spy Camera DVR

.43 | 8 +
US $38.55

Blue Compu

CN)

Produc
Availa st

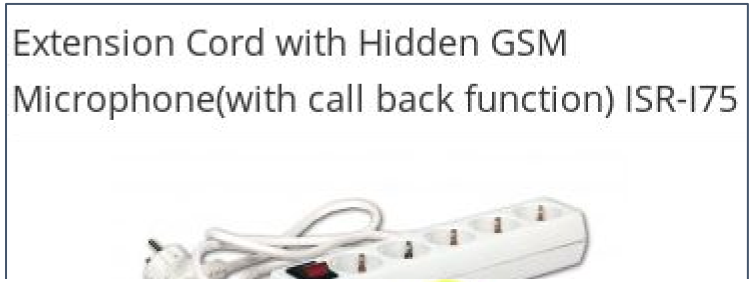
, ships out within 2 business

Pri
$12

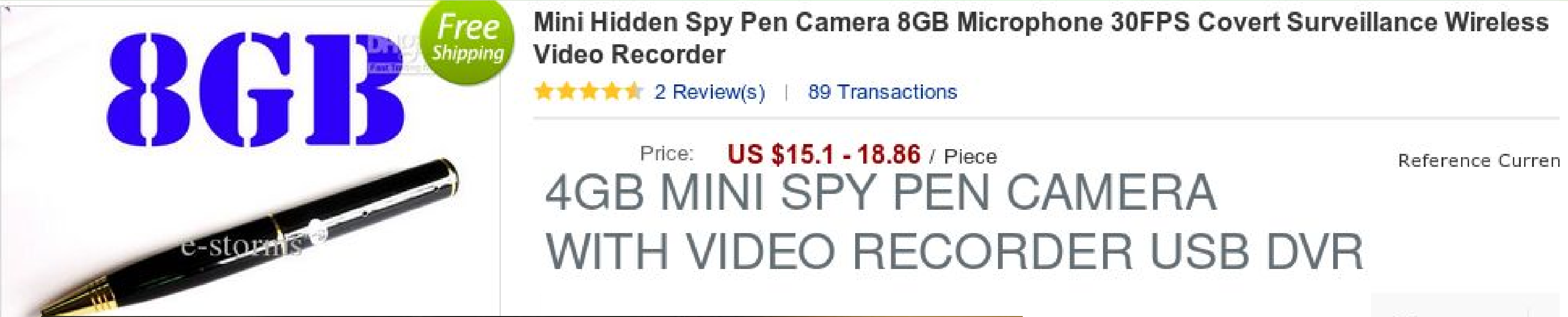
Qty: 1

Like

Spying Devices and How to Plant Them



Extension Cord with Hidden GSM Microphone(with call back function) ISR-I75



Mini Hidden Spy Pen Camera 8GB Microphone 30FPS Covert Surveillance Wireless Video Recorder

★★★★★ 2 Review(s) | 89 Transactions

Price: US $15.1 - 18.86 / Piece

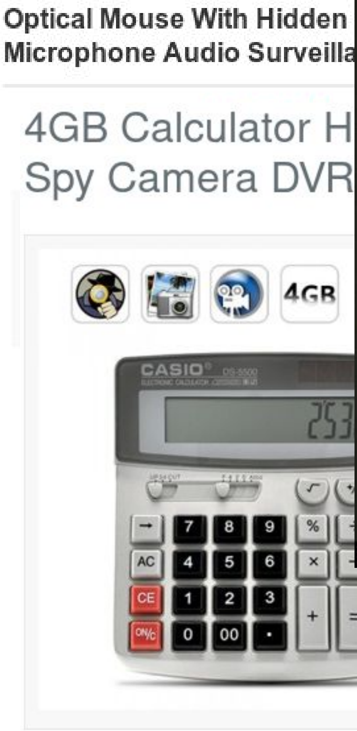
Reference Curren

4GB MINI SPY PEN CAMERA WITH VIDEO RECORDER USB DVR

66 +
US $15.33

Blue Computer & CCTV

Product Code: BL-01
Availability: In Stock



Optical Mouse With Hidden Microphone Audio Surveilla

4GB Calculator H
Spy Camera DVR

© Reuters

SPY HIDDEN GSM BUG/MICROPHONE INMOBILE CHARGER

Spying Devices and How to Plant Them

Extension Cord with Hidden GSM Microphone(with call back function) ISR-I75

Mini Hidden Spy Pen Camera 8GB Microphone 30FPS Covert Surveillance Wireless Video Recorder

★★★★★ 2 Review(s) | 89 Transactions

Price: US $15.1 - 18.86 / Piece

Reference Curren

4GB MINI SPY PEN CAMERA WITH VIDEO RECORDER USB DVR

66 +
US $15.33

Blue Computer & CCTV

Product Code: BL-01
Availability: In Stock

© Reuters

SPY HIDDEN GSM BUG/MICROPHONE INMOBILE CHARGER

Hidden
Microphone
Plant

Hidden
Microphone
Plant
TO LISTEN TO
KEYBOARD
CLACKING
imgflip.com

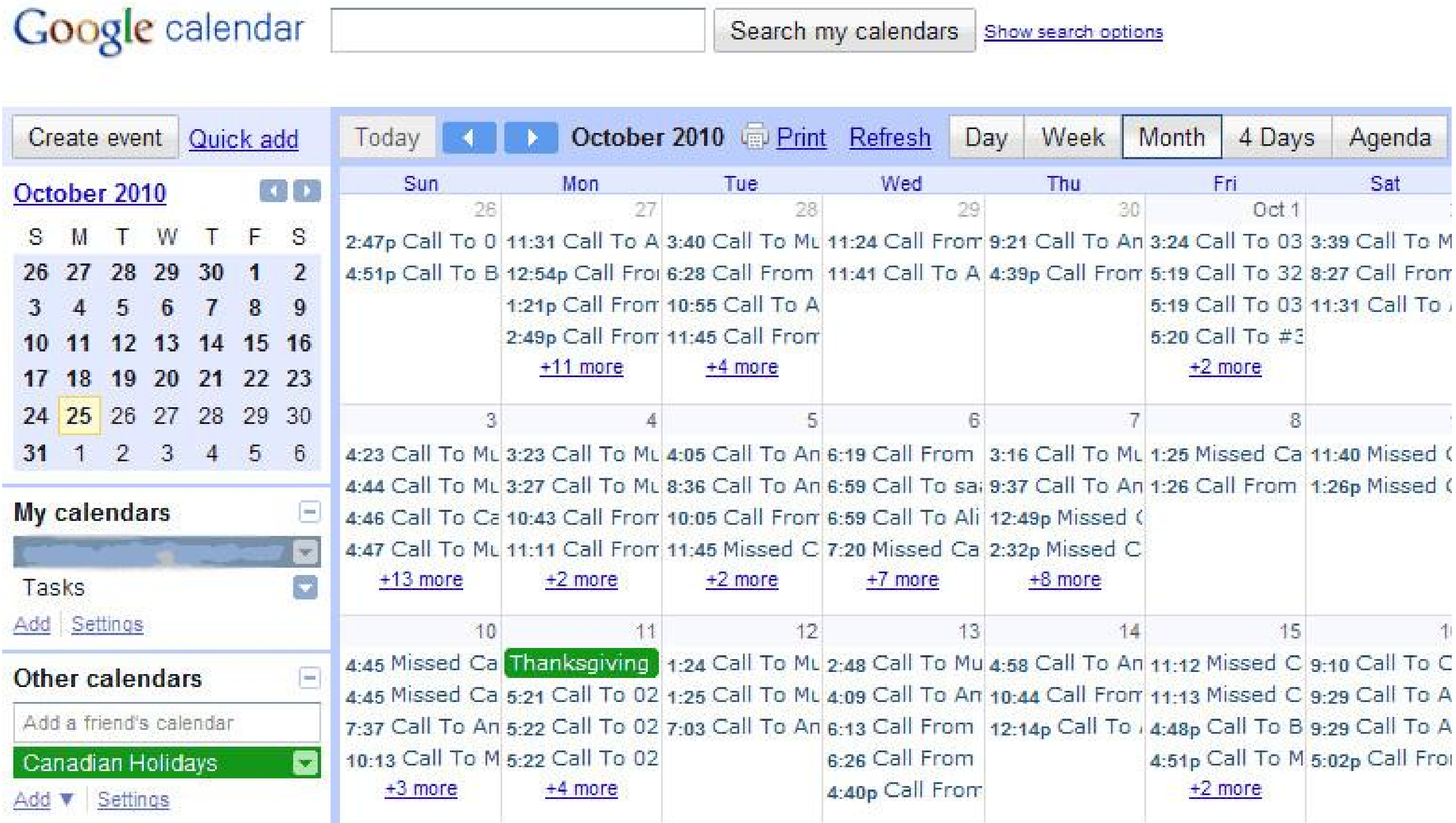
First Takeaway

If I get physical access

I will do worse than plant a bug
to listen to your keyboard

Let’s go remote!

A day in life
of my professors



Google calendar Search my calendars Show search options

Create event Quick add

October 2010

S	M	T	W	T	F	S
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

My calendars

[redacted]

Tasks

Add | Settings

Other calendars

Add a friend's calendar

Canadian Holidays

Add ▼ | Settings

Today ◀ ▶ October 2010 Print Refresh Day Week Month 4 Days Agenda

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	Oct 1	
2:47p Call To 0 4:51p Call To B	11:31 Call To A 12:54p Call Froi 1:21p Call Fron 2:49p Call Fron +11 more	3:40 Call To Mu 6:28 Call From 10:55 Call To A 11:45 Call Fron +4 more	11:24 Call Fron 11:41 Call To A	9:21 Call To An 4:39p Call Fron	3:24 Call To 03 5:19 Call To 32 5:19 Call To 03 5:20 Call To #3 +2 more	3:39 Call To M 8:27 Call Fron 11:31 Call To
3	4	5	6	7	8	
4:23 Call To Mu 4:44 Call To Mu 4:46 Call To Ca 4:47 Call To Mu +13 more	3:23 Call To Mu 3:27 Call To Mu 10:43 Call Fron 11:11 Call Fron +2 more	4:05 Call To An 8:36 Call To An 10:05 Call Fron 11:45 Missed C +2 more	6:19 Call From 6:59 Call To sa 6:59 Call To Ali 7:20 Missed Ca +7 more	3:16 Call To Mu 9:37 Call To An 12:49p Missed (2:32p Missed C +8 more	1:25 Missed Ca 1:26 Call From	11:40 Missed (1:26p Missed (
10	11	12	13	14	15	1
4:45 Missed Ca 4:45 Missed Ca 7:37 Call To An 10:13 Call To M +3 more	Thanksgiving 5:21 Call To 02 5:22 Call To 02 5:22 Call To 02 +4 more	1:24 Call To Mu 1:25 Call To Mu 7:03 Call To An	2:48 Call To Mu 4:09 Call To An 6:13 Call From 6:26 Call From 4:40p Call Fron	4:58 Call To An 10:44 Call Fron 12:14p Call To	11:12 Missed C 11:13 Missed C 4:48p Call To B 4:51p Call To M +2 more	9:10 Call To C 9:29 Call To A 9:29 Call To A 5:02p Call Fro

- Confcalls are *(sometimes)* long and boring

- This motivates multi-tasking
  - *Work still needs to be done*

- So we type stuff

Will it work?

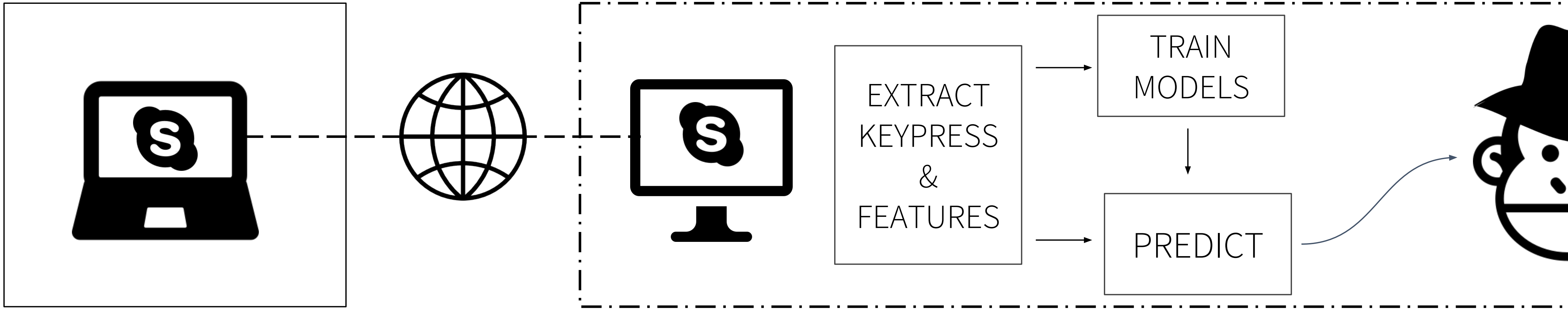
- Not obvious

- VoIP transforms & downgrades audio
  - *MDCT, LPC → sound is almost reconstructed, rather than just encoded*

- Investigate whether key *fingerprints* remain

Attack model

Victim



EXTRACT KEYPRESS & FEATURES

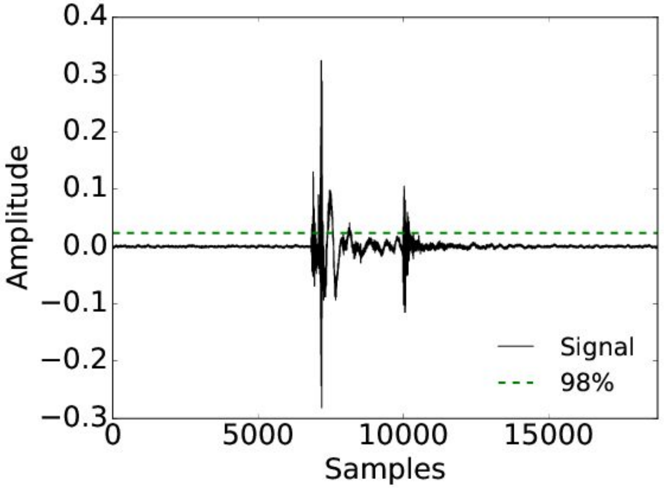
TRAIN MODELS

PREDICT

types *secret*

Practical HOWTO

SEGMENTATION w/THRESHOLDS



→

MEL FREQUENCY CEPSTRAL COEFFICIENTS

→

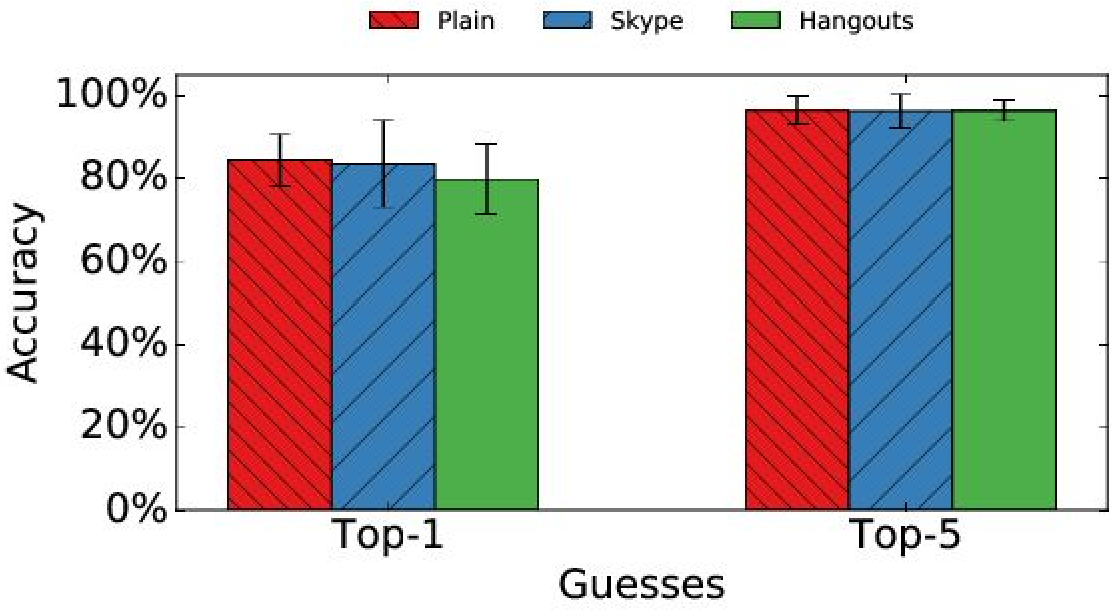
MACHINE LEARNING

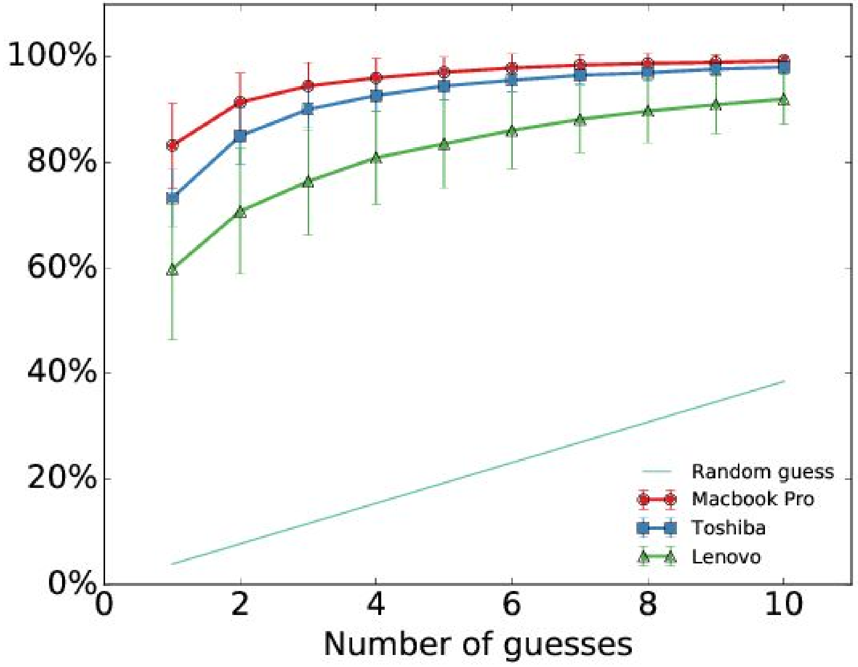
→

DICTIONARY or BRUTEFORCE or GUESSES

Does it work?

Yes.

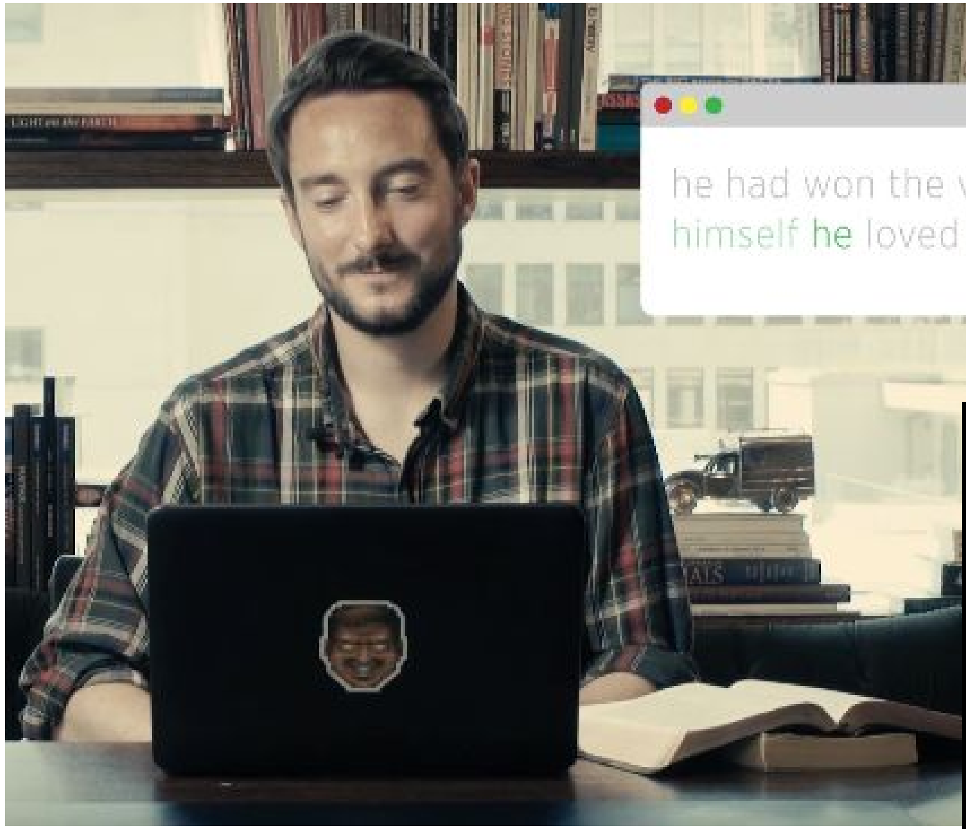




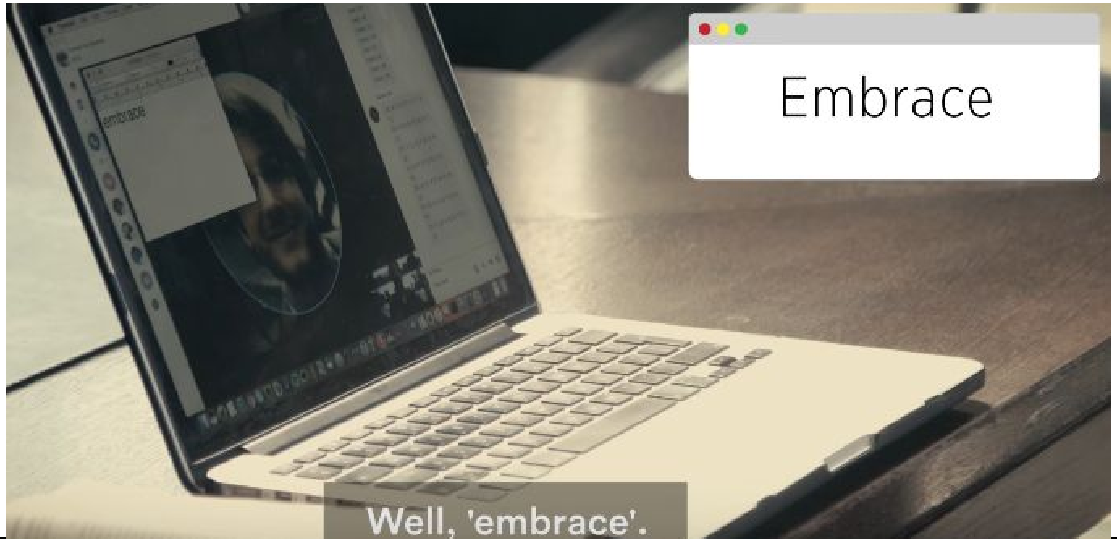
5 volunteers - 3 laptops - typing letters

Does it **really** work?

vs Forbes, 1984 & the Bible

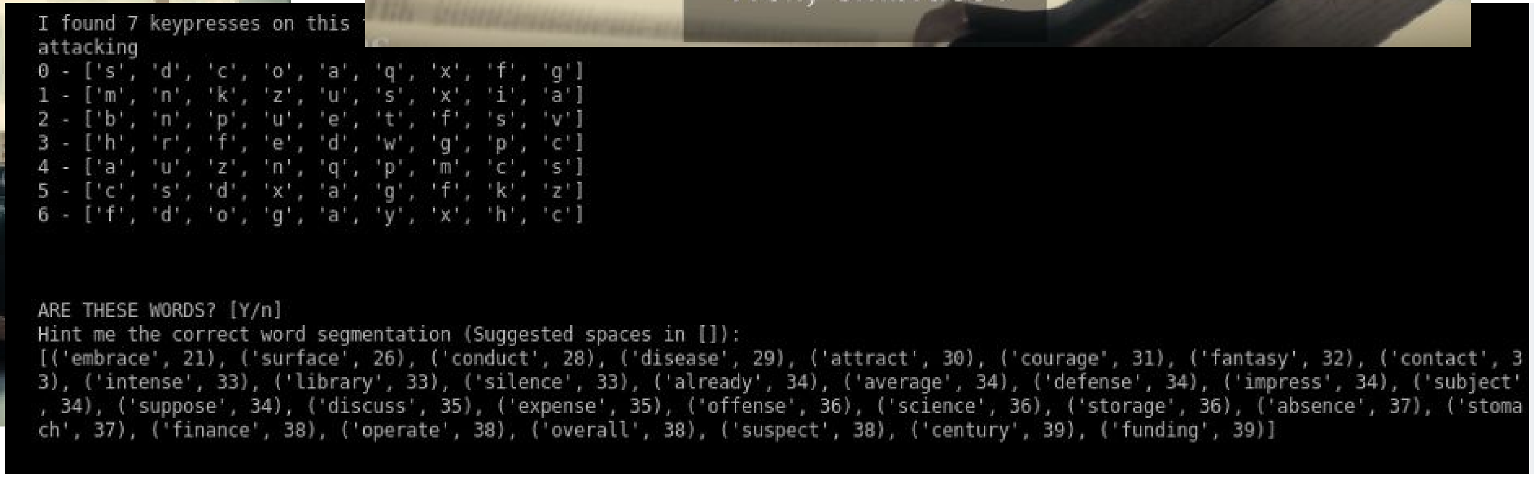


he had won the victory over himself he loved big brother



Embrace

Well, 'embrace'.



```
I found 7 keypresses on this
attacking
0 - ['s', 'd', 'c', 'o', 'a', 'q', 'x', 'f', 'g']
1 - ['m', 'n', 'k', 'z', 'u', 's', 'x', 'i', 'a']
2 - ['b', 'n', 'p', 'u', 'e', 't', 'f', 's', 'v']
3 - ['h', 'r', 'f', 'e', 'd', 'w', 'g', 'p', 'c']
4 - ['a', 'u', 'z', 'n', 'q', 'p', 'm', 'c', 's']
5 - ['c', 's', 'd', 'x', 'a', 'g', 'f', 'k', 'z']
6 - ['f', 'd', 'o', 'g', 'a', 'y', 'x', 'h', 'c']



ARE THESE WORDS? [Y/n]
Hint me the correct word segmentation (Suggested spaces in []):
[('embrace', 21), ('surface', 26), ('conduct', 28), ('disease', 29), ('attract', 30), ('courage', 31), ('fantasy', 32), ('contact', 3
3), ('intense', 33), ('library', 33), ('silence', 33), ('already', 34), ('average', 34), ('defense', 34), ('impress', 34), ('subject'
, 34), ('suppose', 34), ('discuss', 35), ('expense', 35), ('offense', 36), ('science', 36), ('storage', 36), ('absence', 37), ('stoma
ch', 37), ('finance', 38), ('operate', 38), ('overall', 38), ('suspect', 38), ('century', 39), ('funding', 39)]
```

Forbes Credits: https://www.forbes.com/sites/thomasbrewster/2017/07/06/skype-and-type-attack-steals-passwords

Grab The Code

- Open Source tool:

  github.com/SPRITZ-Research-Group/Skype-Type

- Different blocks for audio input, segmentation, learning, and output
  - *Customizable and extensible*

DEMO!

…What could possibly go wrong?

Black Hat Sound Bytes

1. New and surprising extension to the old side-channel, larger attack surface

2. VoIP: an effective and practical means of eavesdropping on keyboard input

3. Don’t Skype & Type :-)

Thanks!

Daniele Lain

daniele.lain3@gmail.com

SPRITZ Group
University of Padua, IT

Daniele Lain

Prof. Mauro Conti

Dr. Alberto Compagno

SPROUT
UC Irvine, USA

Prof. Gene Tsudik

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

SPROUT - Security and Privacy Research OUTfit