DISCOVERING DIGITAL SPYING EYES

MAMPU CIO Convex 5-6 October 2017, Malaysia

Stefanus Natahusada
Kaspersky Lab Singapore

KASPERSKY lab

KASPERSKY lab

SAVING
THE WORLD
FOR 20 YEARS

DIGITAL SPYING EYES – SMART BANDS

Smartbands
what they are and how they work

Components:

1. Bluetooth Module
2. Vibration Motor
3. Motion Sensor
4. Battery
5. Power/Sync Button
6. Power Jack
7. Display

Features:

1. Step counter and approximate distance covered
2. Calorie consumption
3. Sleep recorder (duration and quality)
4. Self-defined fitness plan and a comparison with actual activity
5. Etc

DIGITAL SPYING EYES – SMART BANDS

What data is collected by these devices?

Concerns:

1. What kind of data is being collected
2. What are the risks and where are they?
3. What other parties might be interested in getting hold of this information, what's the potential result?
4. How can users help to protect their data?

Required:

1. Name (or nickname)
2. Birth date (or just birth year)
3. Height
4. Weight
5. Gender
6. E-mail address
7. Password for account

Optional:

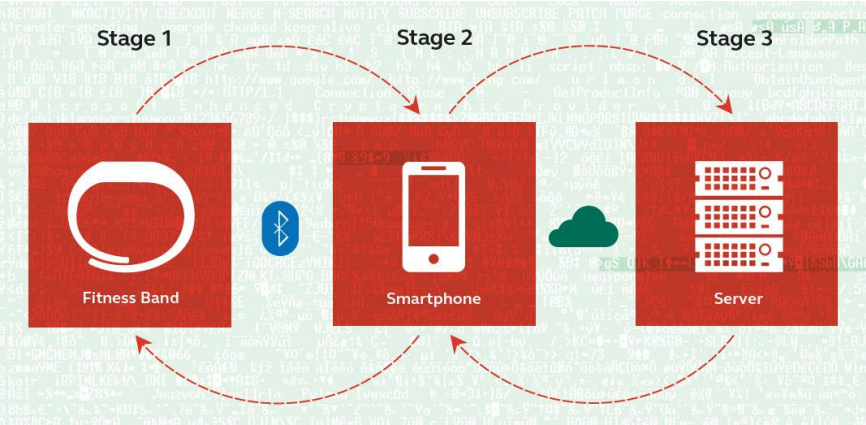
1. Country
2. Training plan
3. Weight goal
4. Training goals (steps per day, hours of sleep)
5. Nutrition plan
6. Photo, Mood
7. Friends using the same fitness tracker

"We entrust fitness trackers with our personal data and invite them into our innermost self"

KASPERSKY lab

DIGITAL SPYING EYES – SMART BANDS

Collecting & Processing Information



Stage 1: Record data and short term storage
Stage 2: Process and correlate data, send instructions to control smartband
Stage 3: long time storage, web based interface for better viewing and deeper investigation

Possible vectors of compromise

1. Synchronization between tracking device & smart phone (blackmail, naming & shaming etc)
2. Synchronization between smart phone & server
3. Compromising the smart phone (mobile malware)
4. Compromising the cloud service (exploit, API etc)
5. Other potential traps (fake apps, scanning Bluetooth-enable devices etc)

DIGITAL SPYING EYES – SMART BANDS

These are the facts, and not so good news:

1. Insurance Companies
2. Employers
3. Advertisement Industry
4. Other Parties

“None of the smart band apps tested offered the opportunity to lock the app with a PIN”

“Personal information gathered by millions of smart band users whets the appetite of cybercriminals”

DIGITAL SPYING EYES – SMART BANDS

Advice for users of smart bands

- Only use features you really need and avoid giving out any personal information that you would not want to store in the cloud
- Use a strong and unique password for each account
- Use security solutions for all devices, if available
- Install app and operating system updates when available
- Uninstall/Delete applications that are not needed anymore
- Etc

DIGITAL SPYING EYES – SMART CITY

Smart Terminals Have Their Weak Points Too

- Parks and streets of modern cities: parking payment terminals, bicycle rental spots etc
- Airports and passenger stations: self-service ticket machines & information kiosks.
- Movie theaters: ticket sale terminals.
- Clinics and public offices: queue management terminals.

Why are those “Smart Terminals” weak?

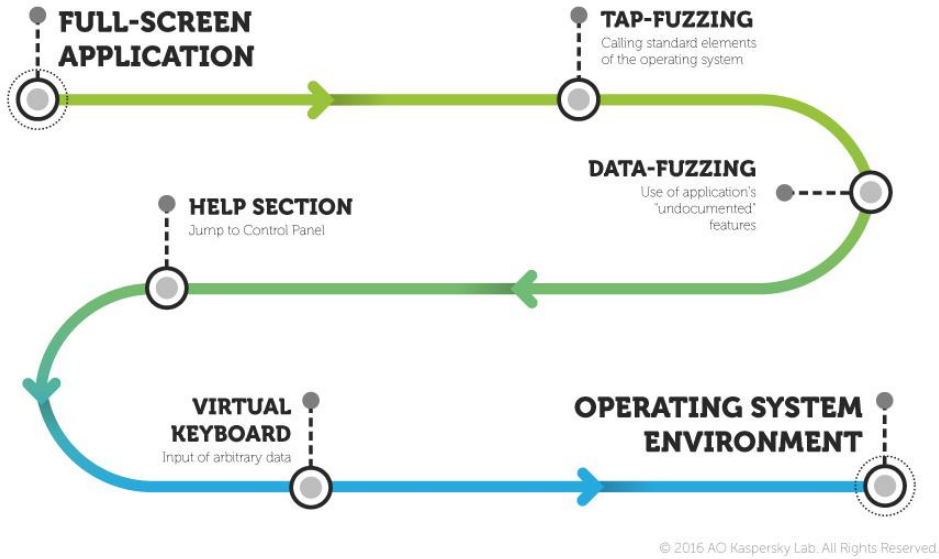
- Many such devices are installed in public places
- It is available 24/7
- It has the same configuration across devices of the same type
- It has a high user trust level
- It processes user data, including personal & financial information
- It is connected to each other, and may have access to other local area networks
- It typically has an Internet connection

DIGITAL SPYING EYES – SMART CITY

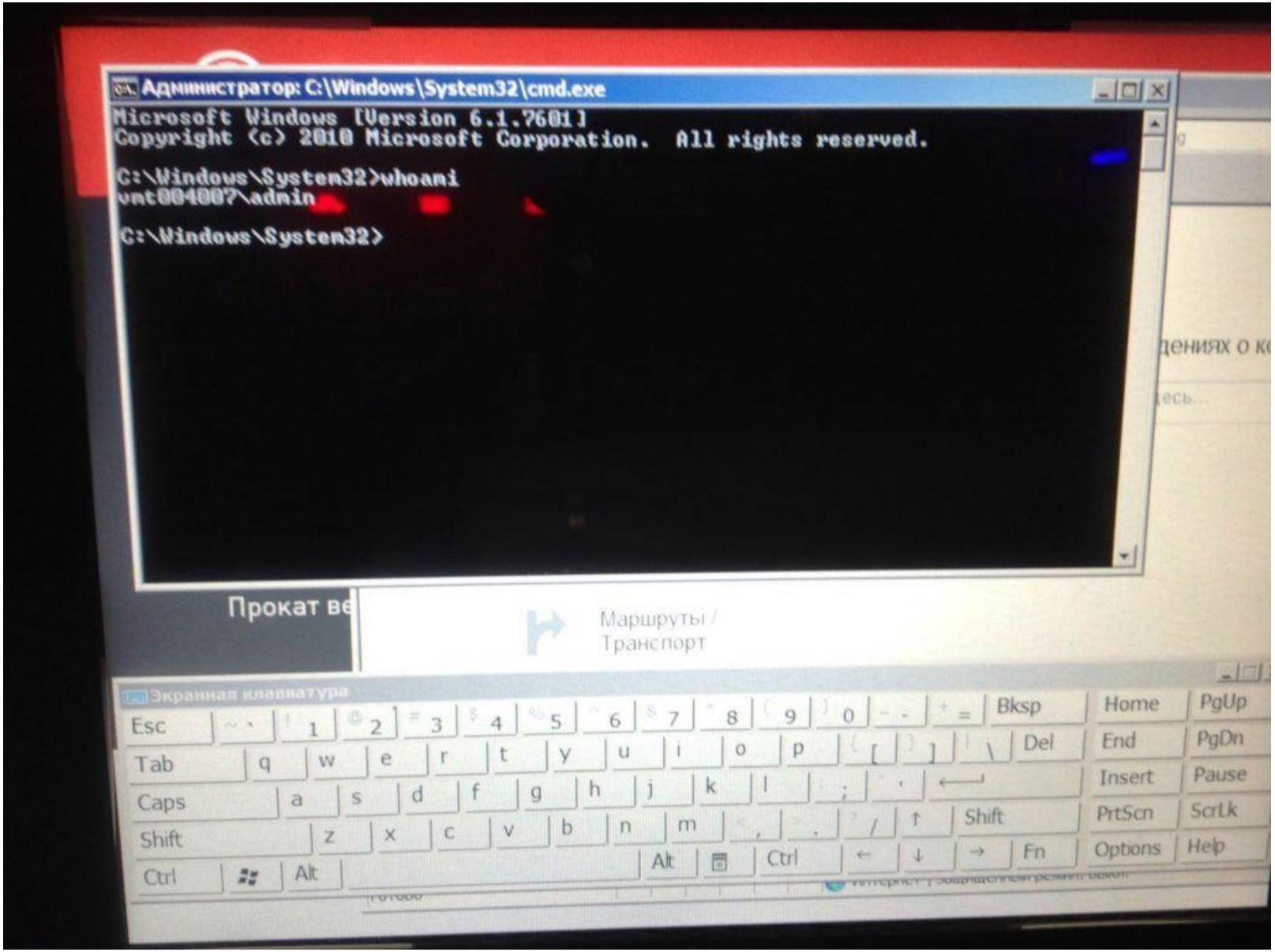
Some Smart City components

1. Touch-screen payment kiosks (tickets, parking etc.)
2. Infotainment terminals in taxis
3. Information terminals at airports and railway terminals
4. Road infrastructure components: speed cameras, traffic routers

Analyzing the security of public terminals



KASPERSKY lab


Администратор: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2010 Microsoft Corporation. All rights reserved.
C:\Windows\System32>whoami
vnt004007\admin
C:\Windows\System32>
Прокат ве
Маршруты / Транспорт
Экранная клавиатура

DIGITAL SPYING EYES – SMART CITY

Recommendations to secure Terminals at public places

1. The kiosk's interactive shell should have no extra functions that enable the operating system's menu to be called (such as right mouse click, links to external sites, etc.)
2. The application itself should be launched using sandboxing technology, such as jailroot
3. Using a thin client is another method of protection. The current operating system session should be launched with the restricted privileges of a regular user – this will make installing new applications much more difficult
4. A unique account with a unique password should be created on each device

DIGITAL SPYING EYES – SMART CITY

Speed Cameras

1. IP address is exposed to the internet
2. Find device with RTSP (Real Time Streaming Protocol)

3. Are there other ports opened?
4. Get access to a database of the registered vehicles

Router

1. Routers use either weak password protection or none at all.
2. Another widespread vulnerability is that the network name of most routers corresponds to their geographic location,
3. These devices are indispensable for the infrastructure of a smart city.
4. Etc

DIGITAL SPYING EYES – SMART CITY

Recommendations to secure Elements of the Road Infrastructure

1. In order protect speed cameras, a full-scale security audit and penetration testing must first be carried out.
2. Another thing that needs to be checked is whether such cameras are assigned an external IP address. This should be avoided where possible.

THANK YOU

KASPERSKY lab