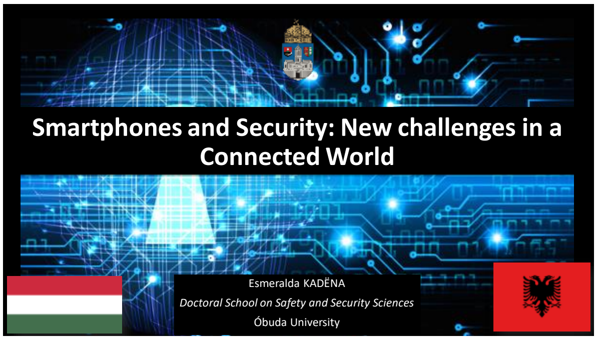
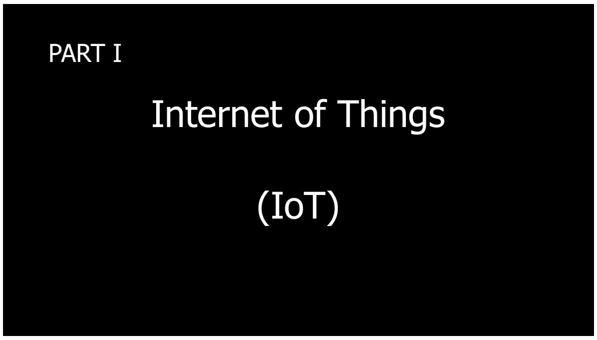


Smartphones and Security: New challenges in a Connected World

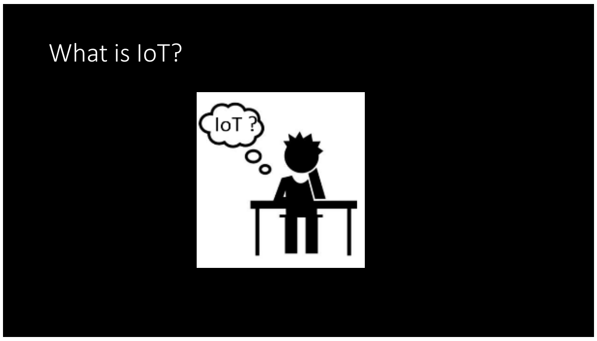
Esmeralda KADËNA
Doctoral School on Safety and Security Sciences
Óbuda University



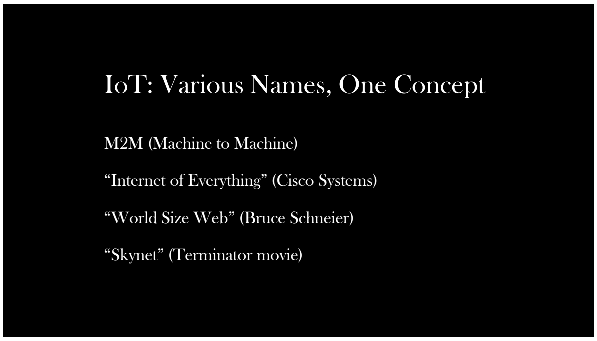
PART I

Internet of Things

(IoT)



What is IoT?



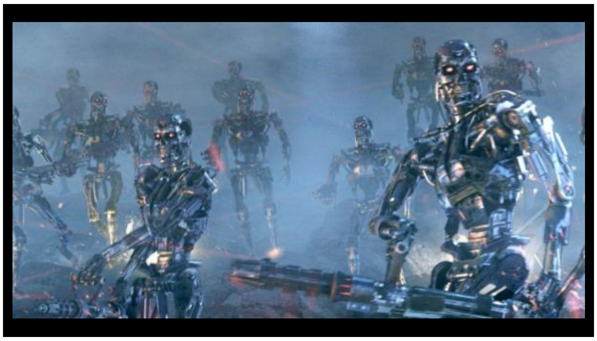
IoT: Various Names, One Concept

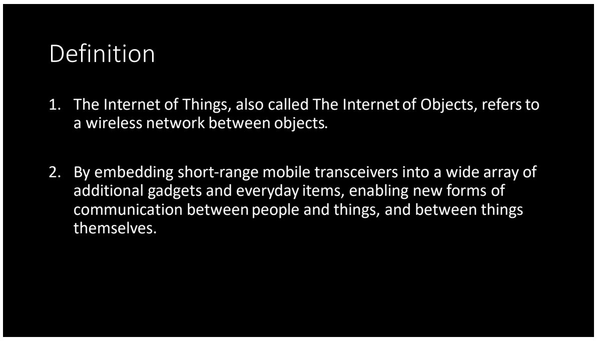
M2M (Machine to Machine)

"Internet of Everything" (Cisco Systems)

"World Size Web" (Bruce Schneier)

"Skynet" (Terminator movie)





Definition

1. The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects.

2. By embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves.

Definition…

3. The term "Internet of Things" has come to describe a number of technologies and research disciplines that enable the Internet to reach out into the real world of physical objects.

4. Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts.

Things?

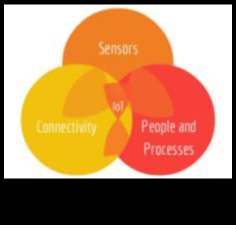
Goods
Objects
Machines
Vehicles
Appliances
Buildings
Animals
Plants
Soil
PEOPLE

Thing

Sight
Smell
Hearing
Touch
Taste

Components of IoT

A combination of:



So…

*“**Sensors and actuators embedded in physical objects are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet.**”*

How did it start?

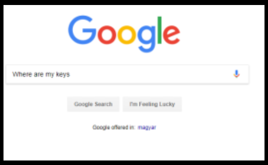
What will we do with that?

1. Connect with THINGS

…new way of interacting with the world!

2. Monitor/Observes

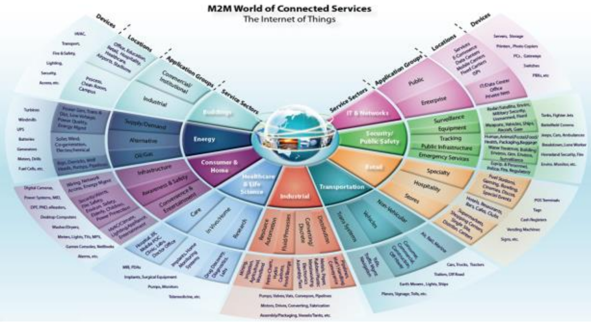
3. Search for THINGS



Where are my keys

Google offered in: magyar

4. Manage THINGS



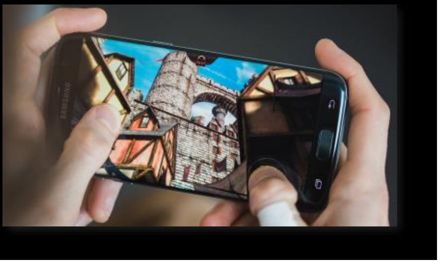
5. Control THINGS

(i.e: Smart Home)

- Automatic control of garage door and gate(s);
- Automatic shut down of appliance when not in use;
- Automatic setting and maintenance of right temperature for each room;
- Automatically adjust/ regulate light intensity based on room luminosity.

6. Play with THINGS

Gaming



The scope of IoT

IoT can connect devices embedded in various systems to the internet.

When devices/objects can represent themselves digitally, they can be controlled from anywhere.

The connectivity then helps us capture more data from more places, ensuring more ways of increasing efficiency.

Corporate aspect

IoT is a transformational force that can help companies improve performance through IoT analytics and IoT Security to deliver better results.

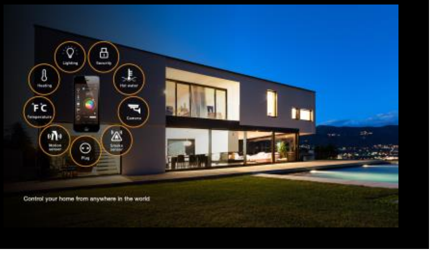
Businesses in the utilities, oil & gas, insurance, manufacturing, transportation, infrastructure and retail sectors can reap the benefits of IoT by making more informed decisions, aided by the torrent of interactional and transactional data at their disposal.

How can IoT help ?

- To organizations: cost reducing through improved process efficiency, asset utilization and productivity.
- The growth and convergence of data, processes and things on the internet would make such connections more relevant and important, creating more opportunities for people, businesses and industries.

Real World Applications of IoT

Smart home

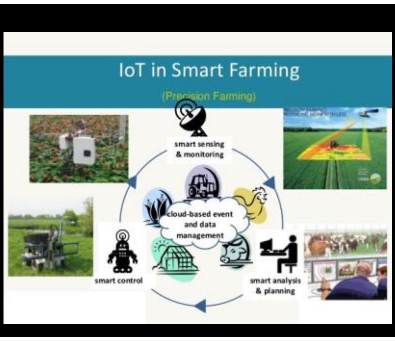


Control your home from anywhere in the world

Wearable devices

Connected cars

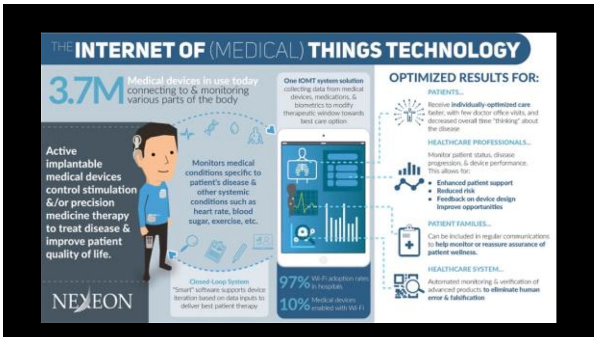
Smart Cities



IoT in Smart Farming

(Precision Farming)

smart sensing & monitoring
cloud-based event and data management
smart control
smart analysis & planning



THE INTERNET OF (MEDICAL) THINGS TECHNOLOGY

3.7M Medical devices in use today connecting to & monitoring various parts of the body

Active implantable medical devices control stimulation &/or precision medicine therapy to treat disease & improve patient quality of life.

Monitors medical conditions specific to patient's disease & other systemic conditions such as heart rate, blood sugar, exercise, etc.

Closed-Loop System
"Smart" software supports device iteration based on data inputs to deliver best patient therapy

One IOMT system solution collecting data from medical devices, medications, & biometrics to modify therapeutic window towards best care option

97% Wi-Fi adoption rates in hospitals

10% Medical devices enabled with Wi-Fi

OPTIMIZED RESULTS FOR:

PATIENTS...
Receive **individually-optimized care** faster, with few doctor office visits, and decreased overall time "thinking" about the disease

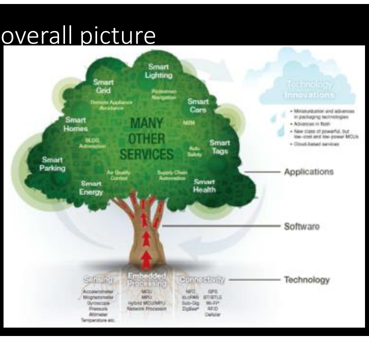
HEALTHCARE PROFESSIONALS...
Monitor patient status, disease progression, & device performance. This allows for:
- **Enhanced patient support**
- **Reduced risk**
- **Feedback on device design improve opportunities**

PATIENT FAMILIES...
Can be included in regular communications **to help monitor or reassure assurance of patient wellness.**

HEALTHCARE SYSTEM...
Automated monitoring & verification of advanced products **to eliminate human error & falsification**

NEXEON

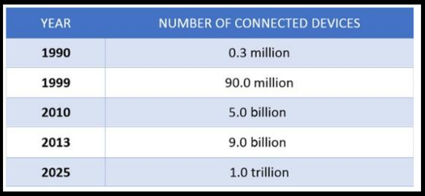
Again- overall picture



WHY???

Why IoT?

- Dynamic control of industry and daily life
- Improve the resource utilization ratio
- Integrating human society and physical systems
- Flexible configuration
- Universal transport & inter-networking
- Acts as technologies integrator



YEAR	NUMBER OF CONNECTED DEVICES
1990	0.3 million
1999	90.0 million
2010	5.0 billion
2013	9.0 billion
2025	1.0 trillion

RISKS

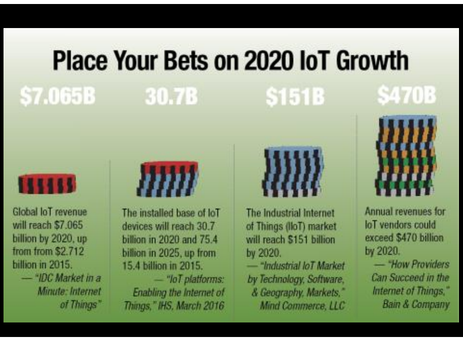
- Connected products are at risk of cyber-attacks
- Impact ranges from inconvenient to catastrophic
- Cyber “hygiene” is essential

Privacy

- Personally identifying information liability
- Privacy breaches will suppress adoption
- Different consumer segments value privacy more/less
- Who owns the data?

Workforce

- New products will require a trained workforce
- Distributors and manufacturers can help educate electricians and other installers



Place Your Bets on 2020 IoT Growth

$7.065B

Global IoT revenue will reach $7.065 billion by 2020, up from from $2.712 billion in 2015.
— *"IDC Market in a Minute: Internet of Things"*

30.7B

The installed base of IoT devices will reach 30.7 billion in 2020 and 75.4 billion in 2025, up from 15.4 billion in 2015.
— *"IoT platforms: Enabling the Internet of Things," IHS, March 2016*

$151B

The Industrial Internet of Things (IIoT) market will reach $151 billion by 2020.
— *"Industrial IoT Market by Technology, Software, & Geography, Markets," Mind Commerce, LLC*

$470B

Annual revenues for IoT vendors could exceed $470 billion by 2020.
— *"How Providers Can Succeed in the Internet of Things," Bain & Company*

PART II

Introduction to Smartphones-history

Why Smartphones?
- Features; - Interesting points, Facts.

Security
- Defining; -Challenges; -Importance; -Malwares and User behavior; -Practical examples; -Discussion.

Protecting yourself

1973: The first cell phone

- The first mobile phone developed by Motorola in 1973.
- It was Martin Cooper who placed the first call at AT&T Bells Labs from the streets of New York.

1984: Nokia Mobira Talkman

- The Phone weighed under 5 kgs and is world's one of the first transportable phones.
- A car and a charger was needed to charge it.
- Once this model was launched, its sales created a stir in the market and the cynics were silenced.

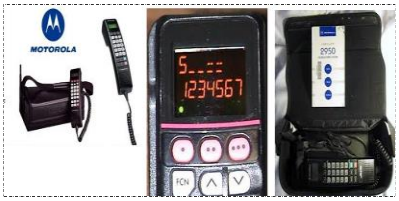
1989: Motorola MicroTac

- Motorola Microtac was the smallest and lightest available phone at that time.
- It was released as the "MicroTac Pocket Cellular Telephone".
- It was designed keeping in mind to fit it in a shirt pocket.

1992: Motorola International 3200

- First digital-sized mobile phone from Motorola introduced in 1992.
- This was the first handset that gave the world an idea of "Flip Phones".

1994: Motorola 2900 BagPhone



- Motorola introduced a very powerful line of mobile phones in 1992.
- These phones put out 3 watts of power (as opposed to 0.6 watts that today's cell phones output) which made them popular for truckers, boaters, and people in rural areas.
- Because of their durability, many of these phones are still in working order today.

1996 – Nokia 8110

•Nokia's first high-end phone was released in 1996

•What made it different was the 'slider' form factor.

•It was made to protect the keypad when kept in pocket and could downslide when in use.

1996 – Nokia 9000 Communicator

- The very first product of the communicator series from Nokia.
- A brand name in the series of business optimized mobile phones.
- On the outside, it appears just like a normal phone & open in clamshell to access the QWERTY keyboard.

For once, we all have played this in our life! -1998

Nokia 5110

- EVERYONE had these!
- Nokia 5110 was the first phone to feature the game snake.
- It had a face plate which allowed users to customize their mobile phone.
- Now mobile phones were not limited to just communication, they were more about fashion now.

1999 – Nokia 8210

- The lightest and smallest available Nokia phone at that time.
- Its selling point was based on the customization and design, with removable X-press on covers.
- Infra-red port for wireless communication.
- SMS (Short Message Service) with predictive text input, with support for major European languages

1999-2002 – RIM BlackBerry 5810

- The Blackberry was first introduced in 1999, but it wasn't until the 2002 model release when users really popped their (Black)Berry, as it featured end-to-end wireless e-mail, print and fax e-mail attachments.
- They were data-only devices, used by professionals, like lawyers, who needed constant access to their e-mail.

2002 – Sanyo SCP - 5300

- In 2002 the first flip-phones were introduced, including the Sanyo SCP-5300, which featured a low-quality camera as well.
- When Sanyo introduced the color-screen SCP-5000 a couple of years ago, consumers got a glimpse of what cell phones might be able to do in the future.

2003 – T-Mobile SideKick

- Paris Hilton wasn't the only one in love with her T-Mobile Sidekick. Users enjoyed a full keyboard behind its swiveling rectangular screen, plus web browsing, e-mail, AOL instant messaging, a cell phone, calendar and camera.
- The Danger Hiptop, also re-branded as the T-Mobile Sidekick, Mobiflip and Sharp Jump is a GPRS/EDGE/UMTS Smartphone produced by Danger Incorporated.
- Real-time e-mail and instant messaging but lacked a speakerphone.

2004 – Motorola Razr V3

- One of the thinnest clamshell phones in the world!
- Half an inch thin and made of anodized aluminum, the Motorola flip phone looks and feels absolutely amazing.
- There's no dispute: The Razr (pronounced "razor") is the coolest-looking phone. Period.

Flip it open, and you're confronted by a vast screen that's bright enough!

2007…

"This will change everything" –Steve Jobs

- This phone completely changed the definition of a Smartphone.
- iPhone is a line of smartphones designed by Apple Inc.
- This phone runs on Apple's iOS mobile operating system.

NOW??
Smartphone era--new millenium

- Strategy Analytics: in 2020 will become available in Japan and South Korea, the first commercial 5G handsets..

…can be followed by the US and China in 2021.

- ~ by 2025, 7% of worldwide mobile connections will be 5G;
- 2010: smartphone sales surpassed PC sales (1st time) (IDC,2010);
- ~ by 2020 the number of mobile phone users will climb to 4.78 billion while the user growth is slowing (eMarketer, 2016);

WHY Smartphones?

- What is a Smartphone?...

No widely agreed definition…

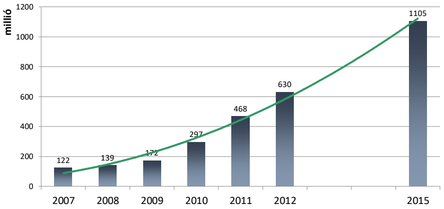
Contains a MNO smartcard with a connection to a mobile network
Phone service and text messaging
Wi-Fi and cellular Internet capabilities (web browsing)
Document storage and productivity capabilities
Different from computers:
-Size
-Functionality

"…a mobile phone that offers more advanced computing ability than a contemporary feature phone…"

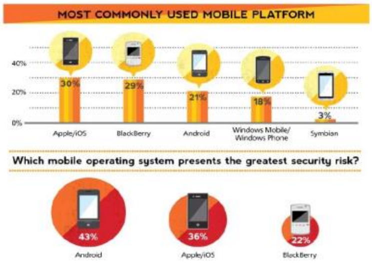
… sorts of things you might expect: iPhones, BlackBerry devices, Android phones, Windows Mobile devices, etc. (all of them have OS) -- pocket size devices that can access the Internet via cellular/3G/4G, WiFi, etc.

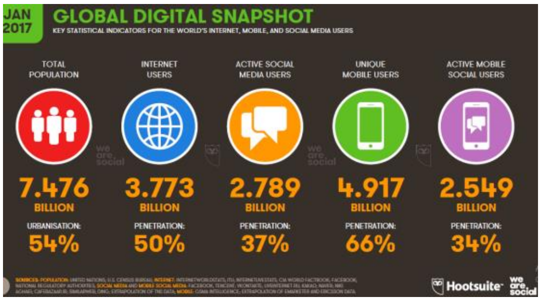
FACTS:

Total Sales

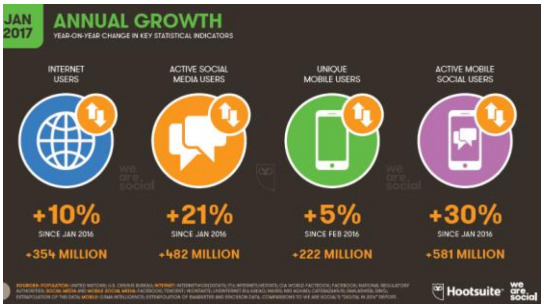


Source: Gartner (April 2011)





Source: We Are Social & Hootsuite (2017)



Source: We Are Social & Hootsuite (2017)

SECURITY

"By failing to prepare, you are preparing to fail."
- Benjamin Franklin

Challenge: Gaining a deeper understanding

Have we learned from the past?

- PCs had(have) many problems
- Smartphone software is different and attempts to address them
- One example is better security features

But are they really better?

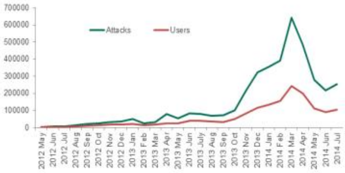
Smartphone Risks

- Increase mobility → Increased exposure
- Easily lost or stolen
  - device, content, identity
- Susceptible to threats and attacks
  - App-based, Web-based, SMS/Text message-based

How do criminals access our information?

1. HACK
2. FOOL
3. STEAL

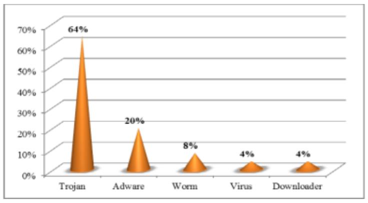
Challenge: Protecting smartphones from attacks



The relationship between the smartphone users and the number of attacks (May 2012-July 2014)

Source: Kaspersky & INTERPOL, "Mobile Cyber Threats Joint Report", 2014

Challenge: Preventing Malware Software



Rates of Malware Software affecting Mobile Operating Systems

Source: CISCO Annual Security Report, 2014

Network connection

- Constantly searching for networks in the past
- War drivers

- Driving in their cars;
- Searching & connecting to all available networks;
- Saving them together, GPS location in a DB.

CHALLENGE… ???

“Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted; none of these measures address the weakest link in the security chain.”

Kevin Mitnick

…

Challenge: HUMAN FACTOR

Past/Recent studies:

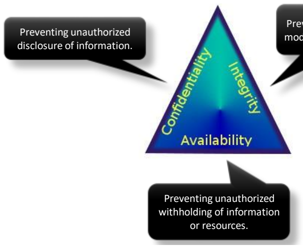
- The appreciation of the mobile device is lower than for desktop PCs-it is more seen as a disposable item (Felt et al., 2012);
- Weak password use, documenting low security awareness, because the relationship between guessable passwords, successful attacks, and the role of the user is often unclear to users (Denning, 1999), (Anderson, 2008);
- 38 % of smartphone users have been victims of cybercrime (Symantec, 2013)

…

…

- Users want to protect their data on smartphone but is not convenient to do it in practice (Boshmaf et.al, 2012);
- Employees compliance with security policies and guidelines is taken for granted in many companies (Onwubiko & Owens, 2012);
- To increase the confidence of user and safety of smartphones a good solution might be upgrading the lock screen system in support of authentication and user’s accessibility and providing suitable security (Muslukhov, 2012).

When talking about privacy…



Preventing unauthorized disclosure of information.

Preventing of unauthorized modification of information.

Confidentiality

Integrity

Availability

Preventing unauthorized withholding of information or resources.

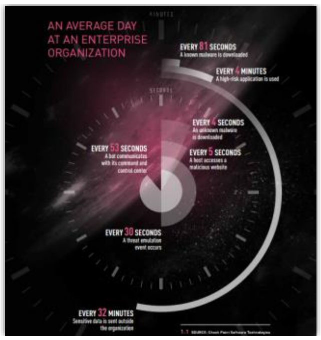
Smartphone security importance

- It stores a plethora of personal information!
- Social media networks, Banking, Hotel Reservation Apps caches data
- An illegitimate access to baseband hardware may result in big blunders

It’s Scary Out There…

Mobile SECURITY means:

The protection of portable devices, such as smartphones, tablets and laptops. Mobile security, also known as wireless security, secures the devices and the networks they connect to in order to prevent theft, data leakage and malware attacks.


AN AVERAGE DAY AT AN ENTERPRISE ORGANIZATION

EVERY 81 SECONDS A known malware is downloaded

EVERY 4 MINUTES A high-risk application is used

EVERY 4 SECONDS An unknown malware is downloaded

EVERY 53 SECONDS A bot communicates with its command and control center

EVERY 5 SECONDS A host accesses a malicious website

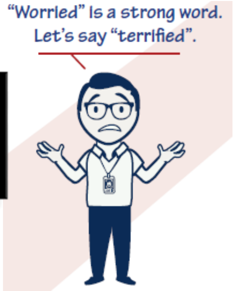
EVERY 30 SECONDS A threat emulation event occurs

EVERY 32 MINUTES Sensitive data is sent outside the organization

1.1 SOURCE: Check Point Software Technologies

Joe IT

Joe IT here already knows a lot about mobile device security. It's his job to secure the corporate network and all of the hardware that runs on it, like laptops and servers.
He's worried about all the smartphones, tablets and other mobile gadgets that are now accessing his precious network and the sensitive business data it protects.

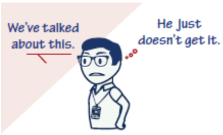


Joe Worker (JW)

JW loves the portability and convenience of mobile computing, and carries his favorite gadget with him everywhere. He wants to use his personal device at work and can't understand why Joe IT shivers at the very idea.

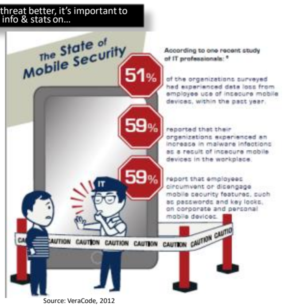
I certainly don't understand the danger here! I mean, it's a smartphone. Nobody attacks mobile phones.

Yup, that's me. I love having my iPad with me at conferences, and it's so much easier to present on it at sales calls.



Joe IT, you can certainly understand why JW loves his iPad. But JW, you need to appreciate that IT organizations are struggling with how to advise employees about securing their smartphone or tablet before it's used as a business tool.
Allowing staff to use any mobile device they choose is becoming a differentiator for companies seeking to hire great employees, but it can become a nightmare for the IT department who is responsible for protecting valuable customer data and company intellectual property (IP).

To understand the threat better, it's important to review some more info & stats on...


The State of Mobile Security

According to one recent study of IT professionals: *

51% of the organizations surveyed had experienced data loss from employee use of insecure mobile devices, within the past year.

59% reported that their organizations experienced an increase in malware infections as a result of insecure mobile devices in the workplace.

59% report that employees circumvent or disengage mobile security features, such as passwords and key locks, on corporate and personal mobile devices.

Source: VeraCode, 2012

- Tend to disturb users by entering at private specific information;
- May cause breakdown of the device and lead to stolen or to become unusable the information/documents of the users;
- Illegal software installed not by the user --used for all attacks that came from the outside taking advantage of the vulnerabilities in the device/system;
- Apple is more protected against OS malware software (thanks to its closed system);
- Android OS --the most target of Malware attacks, because the applications can be taken from many secure-insecure sources.

Way of gathering information:

- Trust (Direct approach, Technical expert)
- The desire to be 'helpful' (Direct Approach, Technical expert, Voice of Authority)
- The wish to get something for nothing (Trojan horse - chain email)
- Curiosity (Trojan horse - open email attachments from unknown senders)
- Fear of the unknown, or of losing something (Popup window)

Way of gathering information…

- Ignorance (Dumpster diving, Direct Approach)
- Carelessness (Dumpster Diving, Spying and eavesdropping)
- Pretexting – (Creating a fake scenario)
- Phishing – (Send out bait to fool victims into giving away their information)
- Fake Websites – (Molded to look like the real thing. Log in with real credentials that are now compromised)

Malware software

Virus

A malicious software which can penetrate into documents and send them elsewhere, distort their contents or making them unusable and make the hardware elements to slow down.

Spyware

They are used to collect information and data regarding a target subject. They specify that their usage is for advertising and promotional purposes (adware) or to offer better service to users (cookies), while what they do is collecting information about a person/organization and send to someone else without their permission (here works like a Trojan)

Trojan

Aims not to spread themselves but to seize the management and the information of the device . Here they differ from worms and viruses. Keyloggers -- transmitted under the cover of a file and the user can unintendedly activate=>the entirely device in the background under control; Not noticed by the user!!!

Worm

A kind of virus but does not require user interaction to reproduce itself. Designed to spread through the network.

Social engineering; SMS, MMS, Phishing.

Real World Scenario:

Recent cyber attack on Bangladesh's central bank that let hackers stole over $80 Million from the institutes' Federal Reserve bank account was reportedly caused due to the Malware (RAT-Remote Access Trojan or a similar form of spyware) installed on the Bank's computer systems and gave attackers the ability to gain control of the bank's computer (thehackenews.com, 2016).

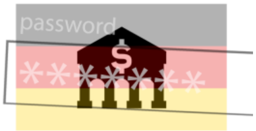
GozNym Banking Trojan (a hybrid of Nymaim and Gozi malware).

- Thrives on carrying out redirection attacks via DNS poisoning;
- Unsuspecting bank customers are redirected to a seemingly legitimate replica of their bank's site and then tricked into giving up their login information.

Target:

- 24 North American banks (April 2016);
- Corporate, SMB, investment banking;
- 17 Polish banks;
- 13 banks and subsidiaries in Germany .

Source: Threatposts, 2016



A virus imbeded in an innocent-looking advert on a website. When clicked, the virus infiltrates users device and monitors every key stroke, even when the user accesses their HSBC bank accounts → extract critical data such as credit card numbers, bank accounts; anything that's of high value (Keiron Shepherd, 2016).

- "This is (manager, director, etc.) and I need…"

- "This is Sue with the Help Desk and we are:
  - verifying your passwords…"
  - troubleshooting logon problems…"
  - got your (bogus) request to change your…"

Social Engineering

The art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques.

Social Engineers use trickery and deception for the purpose of information gathering, fraud, or improper computer system access.

Kevin Mitnick: "The human side of computer security is easily exploited and constantly overlooked".

Social Engineers will:

- Take what little they can find out about you;
- Develop a believable pretext by which to interface with you;
- Drain you of information for their own purposes;
- Complete the con job and disappear;

Types of attacks:

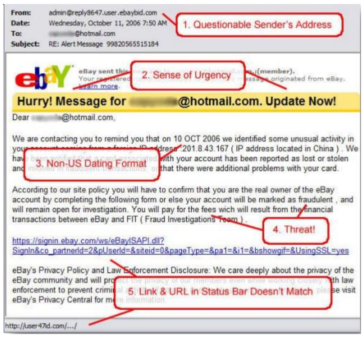
- Attacks by telephone (Trickery through impersonation)
- Attacks by Email / Web Page (“This link/attachment looks legit…let me click it…uh oh!”)
- Attacks in Person (more effective when you don’t know it’s coming)

“Password+Fishing” (Phishing)

Independent from OS and can be used in every type of devices. Attacks are made by directing the user to a false (imitation) website in order to steal private information (credentials, credit card information, user name or password).

Hmm…
I smell something phishy about this!!
Click here…
to verify your bank account information.

Phishing for clicks



From: admin@reply8647.user.ebaybid.com
Date: Wednesday, October 11, 2006 7:50 AM
To: [redacted]@hotmail.com
Subject: RE: Alert Message 99820565515184

1. Questionable Sender’s Address

eBay sent this … (member).
Your registered … message originated from eBay.
Learn more.

2. Sense of Urgency

Hurry! Message for [redacted]@hotmail.com. Update Now!

Dear [redacted]@hotmail.com,

We are contacting you to remind you that on 10 OCT 2006 we identified some unusual activity in your account coming from a foreign IP address 201.8.43.167 (IP address located in China) . We have been notified that a card associated with your account has been reported as lost or stolen and involved in fraudulent transactions, or that there were additional problems with your card.

3. Non-US Dating Format

According to our site policy you will have to confirm that you are the real owner of the eBay account by completing the following form or else your account will be marked as fraudulent , and will remain open for investigation. You will pay for the fees wich will result from the financial transactions between eBay and FIT (Fraud Investigations Team) .

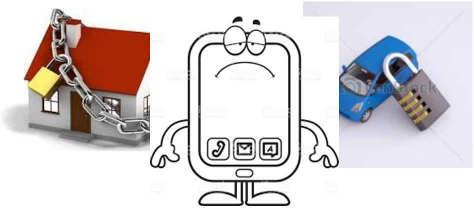
4. Threat!

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&co_partnerId=2&pUserId=&siteid=0&pageType=&pa1=&i1=&bshowgif=&UsingSSL=yes

eBay's Privacy Policy and Law Enforcement Disclosure: We care deeply about the privacy of the eBay community and will protect the privacy of our members even while working closely with law enforcement to prevent criminal … please visit eBay's Privacy Central for more information.

5. Link & URL in Status Bar Doesn't Match

http://user47id.com/…/



Protecting yourself

- Keep in mind: vulnerabilities and attacks will always exist, no matter what operating system you use;
- Trust must be neglected;
- Do not “root” or “jailbreak” the mobile device, you must be careful with third party applications . Always use official application stores to download and install an application;
- The permissions for the installed apps should be checked and if something looks out of order then deny them access;
- Don’t use free or public Wi-Fi, especially when you are accessing sensitive data- connect only in secure wireless connection;
- Beware of Social Engineering techniques;
- Screen lock should be activated;
- A strong password for authentication (a long one is enough);
- Join security trainings and try to gain as much as you can from education.

Information security is the immune system in the body of every organization!!!

Be aware… Connect with care ☺

THANK YOU FOR YOUR ATTENTION !

Questions?

kadena.esmeralda@phd.uni-obuda.hu