Applications Security in IoT

Gabriela Nicolescu
Polytechnique Montréal
gabriela.nicolescu@polymtl.ca

Internet of Things (IoT) Insecurity

- Sheer Scale of IoT implies a new prime target for hackers
- Security is at a very early stage and its grouth is imperative
  - 250 unique security vulenrabilities after testing the 10 most popular IoT products
    - An average of 25 vulnerabilities in each product

(Hewlett-Packard's 2014 IoT Study)

  - 5,000 new mobile malware strains appear every day
    - A new mobile malware strain for Android is discovered every 18 seconds

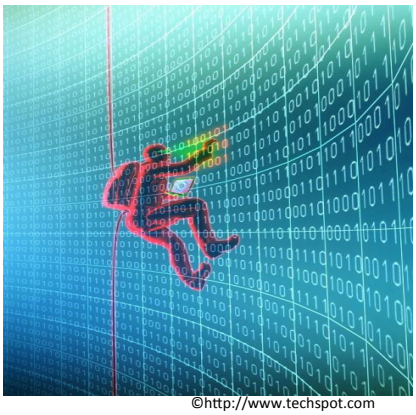
(G DATA and its Q1 2015 Mobile Malware Report)

Internet of Things Units Installed Base by Category
Source: Gartner (november, 2014)

Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2.874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

Hackers vs Security Providers

- Hackers are smart & resourceful
- Hackers are determined and patient
- Hackers have unlimited time
- Hackers do not respects rules
- Sooner or later, any security solution will be reversed
- Recovery from hacking is a must
- Multi-layerd security is required
  - Applications security
  - Hardware security
  - Network security



©http://www.techspot.com

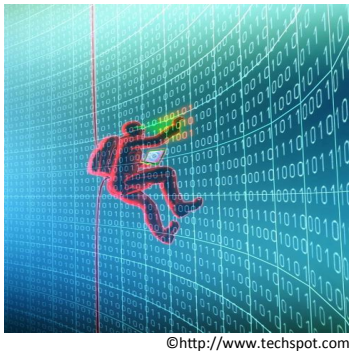
Applications Security

Gartner's one of the top ten technology trends for 2015

- Applications are the leading target of attacks by hackers
- Applications represents security breaches that are not visible to traditional network defense methods
  - Ex.: problems arise when decrypted data is manipulated by applications
- Applications must take a more active role in security to protect themselves
  - Security-aware application design
  - Dynamic and static application security testing
  - Runtime application self-protection, combined with active context-aware and adaptive access controls,
  - Building security directly into the application

Hacking Models

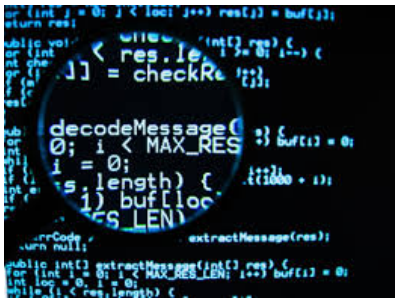
- Static Hacking Model
  - Without launching the target program
    - Ex. of tools: IDA Pro, StudPE, LordPE, ResHacker, RDG Packer Detector, pied
- Dynamic Hacking Model
  - Performed while application is running
    - More flexible and powerful than static models
    - Ex. of tools: IDA Pro , OllyDbg, Immunity Debugger, ProcDump32, ImpRec, LordPE, Frida



©http://www.techspot.com

Debugging

- Hacker's most powerful weapon
  - Total control on memory (execution flow and data) examination
- Once debugger is connected to the application, it is a matter of time for hackers to spot out application vulnerabilities
- OS makers indirectly support hacking
  - Windbg created by Microsoft
  - GDB is open source debugger widely used in Linux systems
  - …



Memory Dump

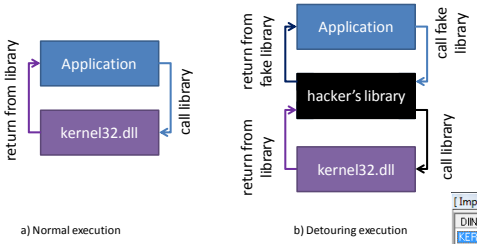
- Powerful dynamic attack
  - copying memory pages (data and code) belonging to the target application
    - Disassembly
    - Memory inspection
- Very easy to implement, using inter-process communication mechanisms
  - SuspendProcess
  - ReadProcessMemory
- Only few functions are necessary to perform this attack

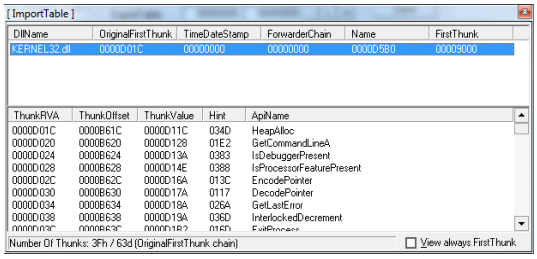
```
#include <windows.h>
#include <iostream>
#include <conio.h>

using namespace std;

int main(
{
    int address = 0x1005194;
    int value;
    DWORD pid;
    HWND hwnd = FindWindow (NULL,"Minesweeper");

    if (!hwnd)
    {
       cout <<"Window not found!";
    }
    else
    {
        GetWindowThreadProcessId (hwnd,&pid);
        HANDLE phandle = OpenProcess (PROCESS_ALL_ACCESS,0,pid);

        if (!phandle)
        {
            cout <<"Could not get handle!";
        }
        else
        {
            ReadProcessMemory (phandle,(LPVOID)address,&value,2,0);
            return 0;
        }
    }
}
```

Code Injection

- Attacker introduce (or "inject") code into an application for many purposes
  - Dynamic library exploits
  - Modifying control flow
  - Arbitrarily modify values in a database through a type of code injection called SQL injection.
  - Install malware or execute malevolent code on a server
  - Privilege escalation to root permissions by exploiting an OS service
  - Attacking web users with HTML/Script Injection
  - …

Code Injection (example – Dynamic Library Exploit)





Secure Applications Design

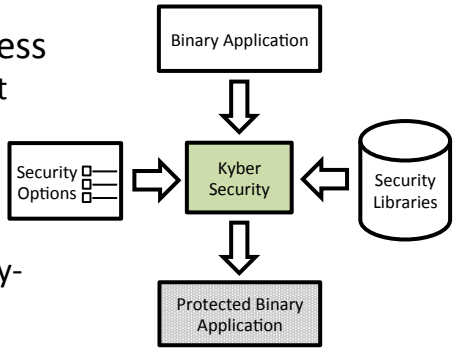
- Developer
  - Algorithms, features
  - Performances
  - Time-to-market
  - Cost
  - ….

- Defender
  - Non-intrusivity
  - Reactivity to threats
  - Performances
  - Accuracy
  - …

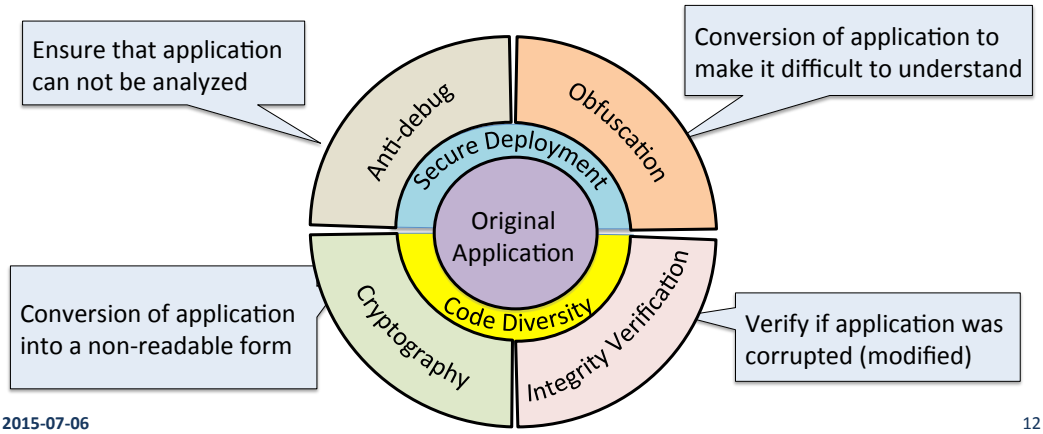
Platforms for secure applications generation are required

Software Security Tool

- Fully automated protection process
  - Easy to integrate into development flow
    - Binary-level protection
    - Compiler/linker independent
    - No prior security knowledge
  - Security options to tune up security-performance trade-off
- Demonstrated on several varied applications



Technology Overview



KyberSecurity Features

Attack Model	Anti-Debug	Integrity Verification	Code Diversity	Cryptography	Obfuscation		
					Resource Concealer	Secure Deployment	Control Flow Concealer
Interactive debugging	★★★★	★	★	★★	★	★	★
Code lifting	★		★★★	★★★★	★★	★	★★★
Run-time memory inspection	★★★★		★★★	★★★	★★★	★★	★★★★
Control flow modification		★★★★	★★	★		★	★★★
Instruction replacement	★	★★★★	★★★	★		★	★★
Dynamic library exploits		★★★	★		★★★★		
Disassembly	★★★		★★★★	★★★	★	★★	★★★★
Reverse Engineering	★★★★		★★★★	★★★	★★★	★★	★★★
Data/resource replacement	★★★★	★★★	★★★	★★★	★★★	★★★	
Automatic attacks	★★★★	★★★	★★★★	★★	★★★★	★★	★★★
Differential attacks	★		★★★★	★★★	★	★★	★★

Technology Assessment

Application name	Application type
Space Bubbles	Game – http://www.myrealgames.com/genres/windows-7-games
Billiard Masters	Game – http://www.myrealgames.com/genres/windows-7-games
Adobe Reader	PDF file reader
FoxitReader	PDF file reader
write	Windows provided text editor
Notepad++	Advanced text editor
Winword (2007)	Microsoft Office text editor
Powerpoint (2007)	Microsoft Office presentation
Outlook (2007)	Microsoft Office email
Immunity debugger	Debugger
OllyDbg	Debugger
XDbg	Debugger
ProcessHacker2	Multi-purpose tool to monitor system resources
Elecard Suite Tools	Multimedia – H264 tools development
CanyEdgeDetector	Computer Vision Algorithm
cygwin-ssh	ssh provided by Cygwin installation

Security Audit

- Performed by two independent security audit companies
- Security tests performed
  - Automatic test penetration
  - Static and dynamic attacks
  - Reverse engineering
- Attacks duration
  - 9 hours - No failure
  - 8 days - Failure only for memory dumping
    - An improvement was performed following the audit

Conclusions

- Information security has never been more challenging
- Application security is one of the areas of concern in cloud computing
  - Advanced threats to be considered
  - Automatic protection
- KyberSecurity platform for software protection
  - Automatic security protectors insertion starting from the binary of the original application
  - High level security
  - Performance

Technology protected by patent (#19309180)