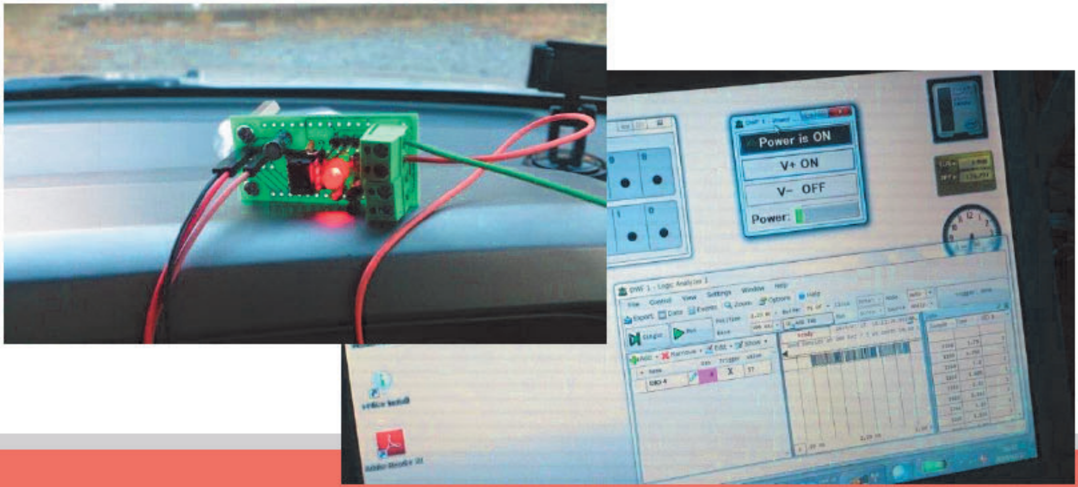
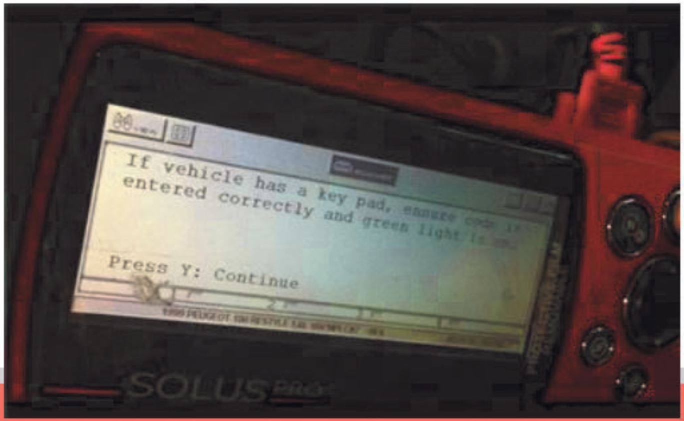
Threat Analysis on Windows 10 IoT Core and Recommended Security Measures

FFRI Inc.

About Myself

- Formerly worked as a network engineer involved in quality assessment of multilayer switches and firmware development (missionary of automation using IXIA and the necessity of regression test around 2007).
- Joined FFRI in 2013. Involved in development of a driver protection system using Type 1 VMM, assessment of embedded systems and development of a prototype of a 0-day protection system.
- Since 2015 involved mainly in research of automobile security.




If vehicle has a key pad, ensure code is entered correctly and green light is on.

Press Y: Continue

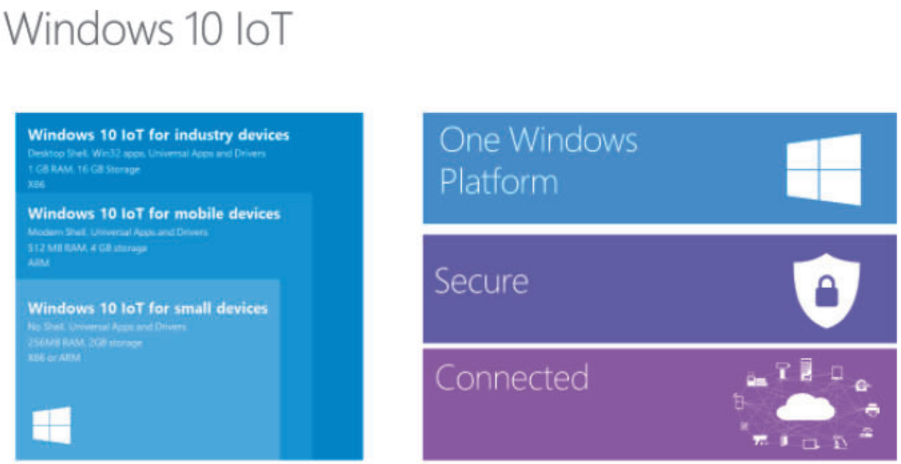
Agenda

- Windows 10 IoT Core Overview
- Standard Security Feature of Windows 10 IoT Core
- Attack Vector & Threat Analysis
- Recommended Security Measures for Windows 10 IoT Core
- Summary

Windows 10 IoT Core Overview

From Embedded to IoT

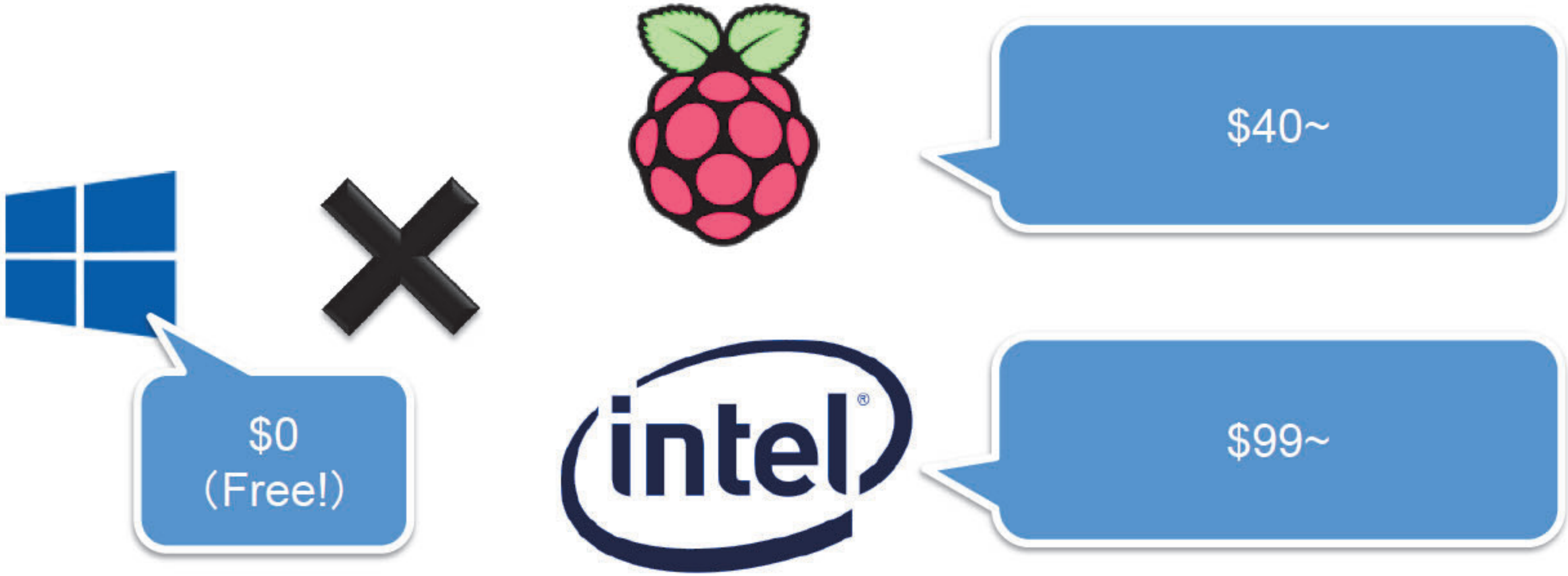
- Windows Embedded series has been renewed to Windows IoT series along with the release of Windows 10.
- Windows 10 IoT Core is the smallest of the Windows series targeting sensors and small devices.


Windows 10 IoT
Windows 10 IoT for industry devices
Desktop Shell, Win32 apps, Universal Apps and Drivers
1 GB RAM, 16 GB Storage
X86
Windows 10 IoT for mobile devices
Modern Shell, Universal Apps and Drivers
512 MB RAM, 4 GB storage
ARM
Windows 10 IoT for small devices
No Shell, Universal Apps and Drivers
256MB RAM, 2GB storage
X86 or ARM
One Windows Platform
Secure
Connected

http://az648995.vo.msecnd.net/win/2015/03/IoT-1.png

Windows OS supports SBC as well

- Windows 10 IoT Core can be used with SBC(Single Board Computers) such as Raspberry Pi 2 and Intel's MinnowBoard MAX (free).



Standard Security Features of Windows 10 IoT Core

Windows 10 IoT Core vs. Desktop Version

Supported by Windows 10 IoT Core

- DEP
- ASLR
- Control Flow Guard *Requires an option upon build
- Windows Firewall *Customization expected

Not Supported by Windows 10 IoT Core

- Windows Update
- Windows Defender
- User Account Control

Still no support for Windows Update after 2 months... We've investigated if there is no problem along.

Microsoft's Security Updates(Aug. – Sept.)

- Security Updates for Windows 10
  - Windows 10 Systems
    - MS15-080, MS15-085, MS15-088, MS15-091, MS15-097, MS15-098, MS15-102, MS15-105
  - Microsoft .NET Framework
    - MS15-080(3.5), MS15-092(4.6), MS15-101(3.5/4.6)
  - Internet Explorer 11/Microsoft Edge
    - MS15-079, MS15-091, MS15-093, MS15-094, MS15-095

Excluded because Windows 10 IoT Core does not include Internet Explorer / Edge

Microsoft's Security Updates(Aug. – Sept.)

- Security Updates for Windows 10
  - Windows 10 Systems
    - MS15-080, MS15-085, M
      MS15-097, MS15-098, M

Excluded because Windows 10 IoT Core uses CoreCLR, a subset of .NET Framework
and it causes no direct effect

  - Microsoft .NET Framework
    - MS15-080(3.5), MS15-092(4.6), MS15-101(3.5/4.6)
  - Internet Explorer 11/Microsoft Edge
    - MS15-079, MS15-091, MS15-093, MS15-094, MS15-095

Microsoft's Security Updates(Aug. – Sept.)

- Security Updates for Windows 10
  - Windows 10 Systems
    - MS15-080, MS15-085, MS15-088, MS15-091, MS15-097, MS15-098, MS15-102, MS15-105
  - Microsoft .NET Framework
    - MS15-080(3.5), MS15-
  - Internet Explorer 11/Microsoft Edge
    - MS15-079, MS15-091, MS15-093, MS15-094, MS15-095

Some patches like MS15-102 (Privileges Escalation exploiting a vulnerability in Task Manager) affects both Windows 10 and IoT Core but not all of them do due to a difference in architecture.

Attack Vector & Threat Analysis

Research on Network Services

- We researched the possibility of remote attacks.
- Some ports were found to be open by default through scanning TCP/UDP ports.
- We focused on ports for FTP and the remote debugging service, ports that are thought to be most common for attacks.

Research on Network Services (cont.)

- Below are the ports that are open by default and command lines given to their executables.

Port No.	Nmap's guess	Command Line
21.tcp	ftp	ftpd.exe
22.tcp	ssh	C:¥windows¥System32¥svchost.exe -k SshSvcGroup
135.tcp	msrcp	C:¥windows¥system32¥svchost.exe -k RPCSS
445.tcp	microsoft-ds?	System
4020.tcp	trap?	C:¥RDBG¥msvsmon.exe /CHILDSERVER 188 "+:4020" {5D8A1EE3-3C96-4562-AD8A-8E4740A26577} 0x3 148 140 13c 144 /silent- /servicemode-
5985.tcp	wsman?	System
8080.tcp	http-proxy	System
9955.tcp 9955.udp	unknown	C:¥windows¥system32¥svchost.exe -k LocalService
47001.tcp	unknown	System

Research on Network Services (cont.)

- The services we observed are meant for these purposes.

Port No.	Nmap's guess	Command Line
21.tcp	ftp	
22.tcp	ssh	
135.tcp	msrcp	
445.tcp	microsoft-ds?	System
4020.tcp	trap?	C:¥RDBG¥msvsmon.exe /CHILDSERVER 188 "+:4020" {5D8A1EE3-3C96-4562-
5985.tcp	wsman?	
8080.tcp	http-proxy	
9955.tcp 9955.udp	unknown	
47001.tcp	unknown	System

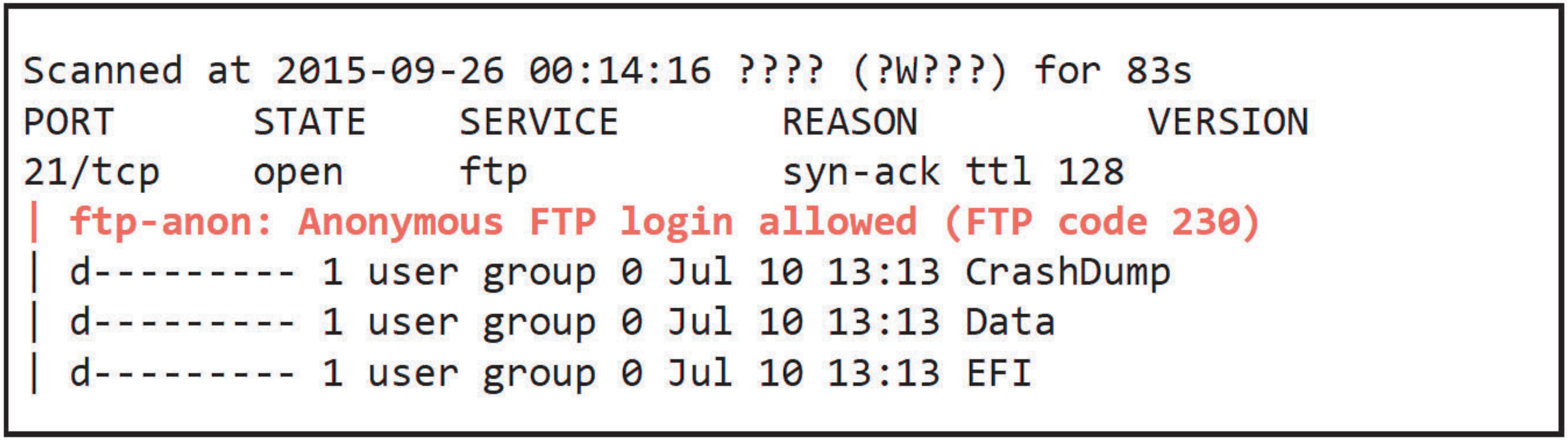
MS's official webpage describes a way to edit startup files using FTP.

Although Nmap's guess was trap, this is actually used by Visual Studio 2015 for remote debugging. This is registered in Task Scheduler and will automatically halt after a certain time.

…Does FTP require no authentication?

- Nmap’s result tells us that the default FTP service allows an anonymous login.

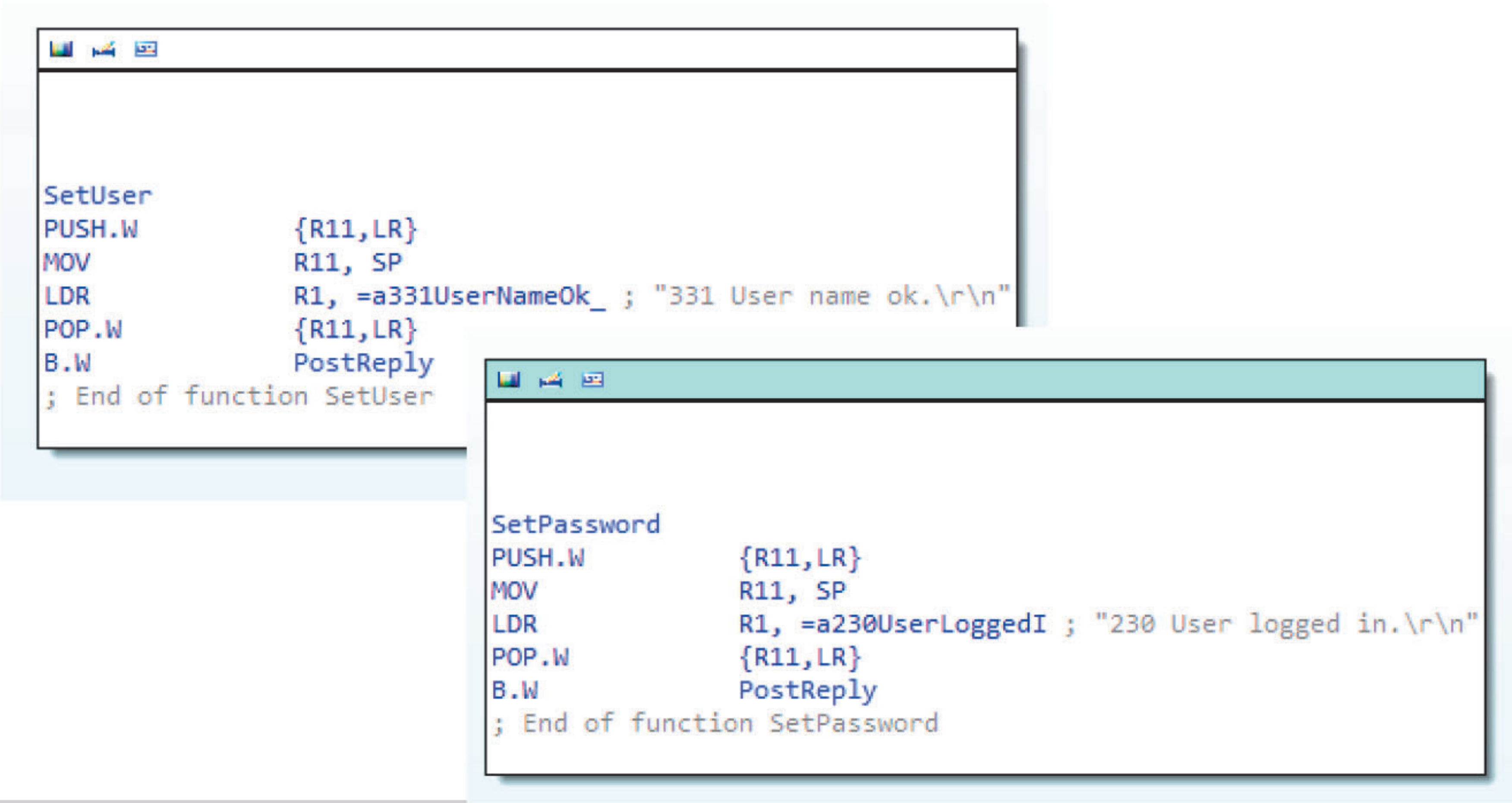
- The banner output differs from what traditional Windows would output. Therefore we’ve observed its binary.



```
Scanned at 2015-09-26 00:14:16 ???? (?W???) for 83s
PORT      STATE    SERVICE        REASON          VERSION
21/tcp    open     ftp            syn-ack ttl 128
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| d--------- 1 user group 0 Jul 10 13:13 CrashDump
| d--------- 1 user group 0 Jul 10 13:13 Data
| d--------- 1 user group 0 Jul 10 13:13 EFI
```

…FTP required no authentication, for real

- Analyzing ftpd.exe told us that there’s no authentication logic!



```
SetUser
PUSH.W          {R11,LR}
MOV             R11, SP
LDR             R1, =a331UserNameOk_ ; "331 User name ok.\r\n"
POP.W           {R11,LR}
B.W             PostReply
; End of function SetUser
```

```
SetPassword
PUSH.W          {R11,LR}
MOV             R11, SP
LDR             R1, =a230UserLoggedI ; "230 User logged in.\r\n"
POP.W           {R11,LR}
B.W             PostReply
; End of function SetPassword
```

Summary of the FTP Service

- The FTP service in Windows 10 IoT Core has no authentication feature.
  - We cannot add an authentication later.

- The FTP service is written in the startup file so it will always start at device boot.

- Default root directory is set at “C:¥”.
  - It is possible to overwrite some files under “C:¥RDBG” and “C:¥Windows¥System32¥” which contain files related to the remote debugging service.

…Does Remote debug "also" require no authentication?

- As with the FTP service, the remote debugging feature available since VS2015 also requires no authentication by default.

- Configurations regarding remote debugging are also written in the startup file and it intentionally disables some security-related configurations.

```
schtasks /create /f /tn "StartMsvsmon" /tr "%SystemDrive%¥RDBG¥msvsmon.exe
     /nowowwarn /noauth /anyuser /nosecuritywarn /timeout:36000" /ru
                DefaultAccount /sc onstart >nul 2>&1
```

Web UI

- By default Windows 10 IoT Core has a built in web UI like other standard IoT devices do.

- Unlike the FTP and the remote debug, accesses to the web UI goes through Basic authentication. However, it is HTTP by default.

- Some actions can be done through REST API.
  - Documents are available at /RestDocumentation.htm

- The Web UI allows for a deployment of applications and some configurations of the device, but does not allow for security-related configurations that we recommend today.

Research on Attack Scenario

- We’ve examined the anticipated threats upon 3 elements: Confidentiality(C), Integrity(I) and Availability(A).
- We’ve also considered malwares that would exploit these threats.
- Lastly, we’ve created a diagram that clarifies relationships between these threats.

Threats against Confidentiality(C)

- Sniffing/Password cracking （or Steal）
  - Since the web UI uses HTTP + Basic authentication by default, passwords can be stolen by intercepting packets.
  - Like we've seen in attacks against home routers, there is a chance that password cracking will be attempted against services like HTTP and SSH.
- Unauthorized access/Spoofing
  - Since there is no setup wizard on initial setup, one may operate the system with the built in account left set with the default password.

Threats against Integrity(I)

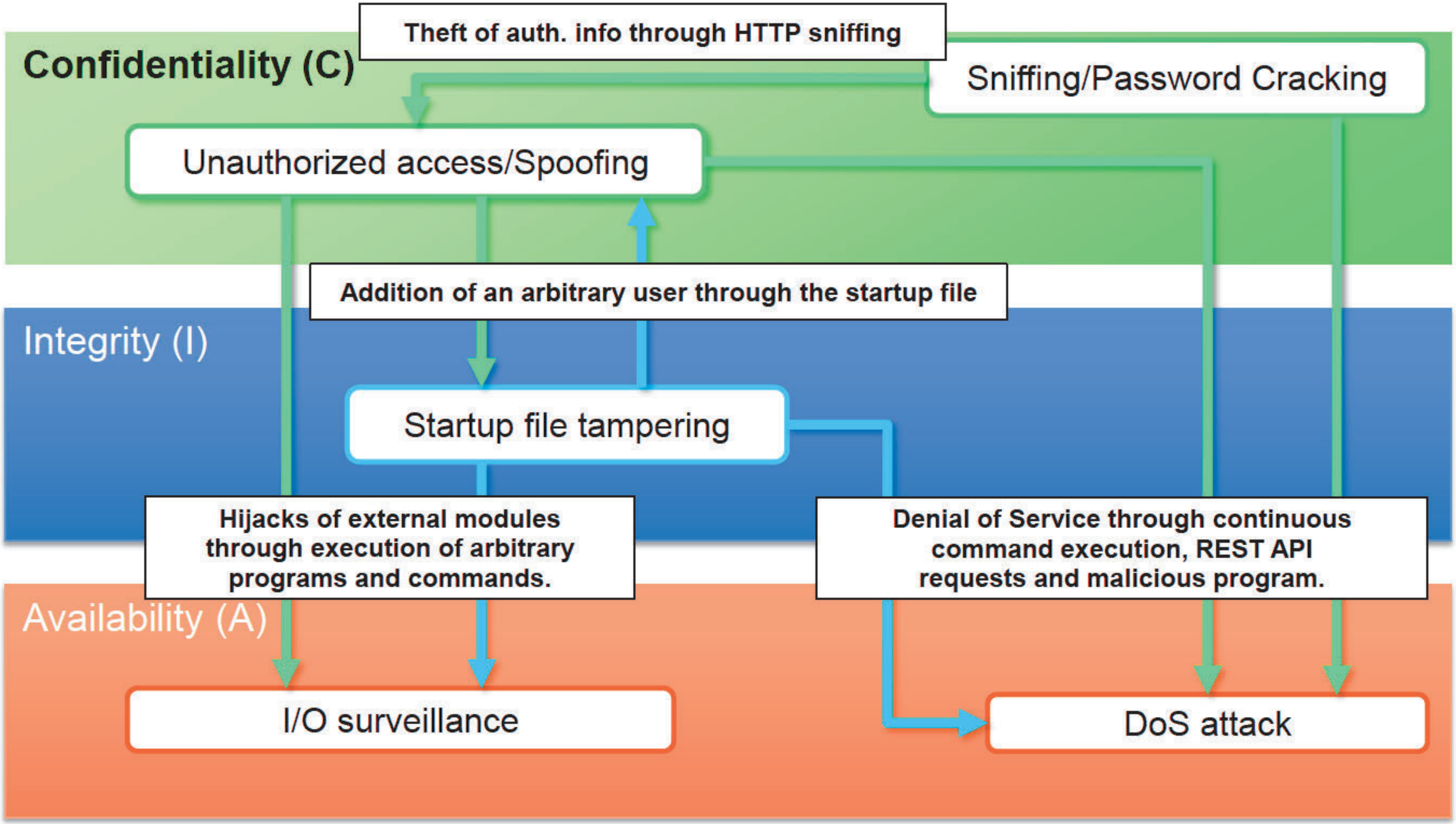
- Startup file tampering
  - By exploiting the FTP service on default configuration, an attacker can overwrite the startup file.
  - Since the startup file gets executed as a batch file, it is possible to create a new arbitrary user by the “net use” command.

Threats against Availability(A)

- DoS Attack
  - Attempts on password cracking and continuous REST API request can eventually cause a Denial of Service.

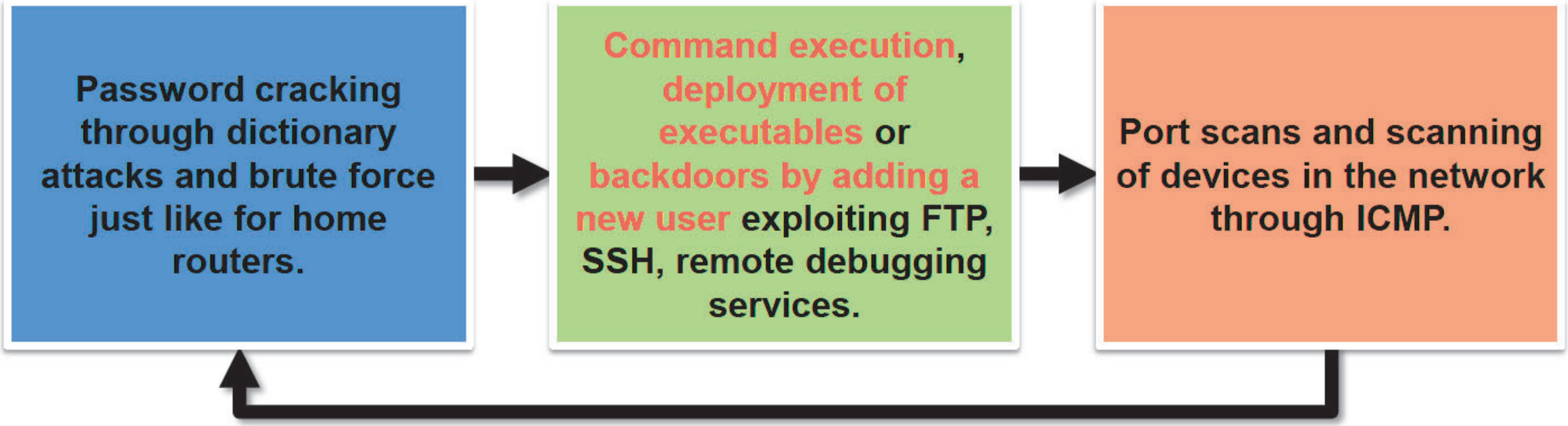
- I/O surveillance
  - Malicious accesses and spoofing may allow for unauthorized use of camera modules connected to the device(secret photography) or operation of sensors.

Relationships between Threats


Theft of auth. info through HTTP sniffing
Confidentiality (C)
Sniffing/Password Cracking
Unauthorized access/Spoofing
Addition of an arbitrary user through the startup file
Integrity (I)
Startup file tampering
Hijacks of external modules through execution of arbitrary programs and commands.
Denial of Service through continuous command execution, REST API requests and malicious program.
Availability (A)
I/O surveillance
DoS attack

These threats are very likely to be exploited by malwares

- The threats in the default system are very analogous to the threats in embedded devices like home routers.
  - Chance of being operated with default accounts.
  - No encryption to the web UI.
  - FTP and remote debugging service without authentication.
- Therefore, there is a very high chance of being targeted by worms that would repeat an intrusion and an infection.



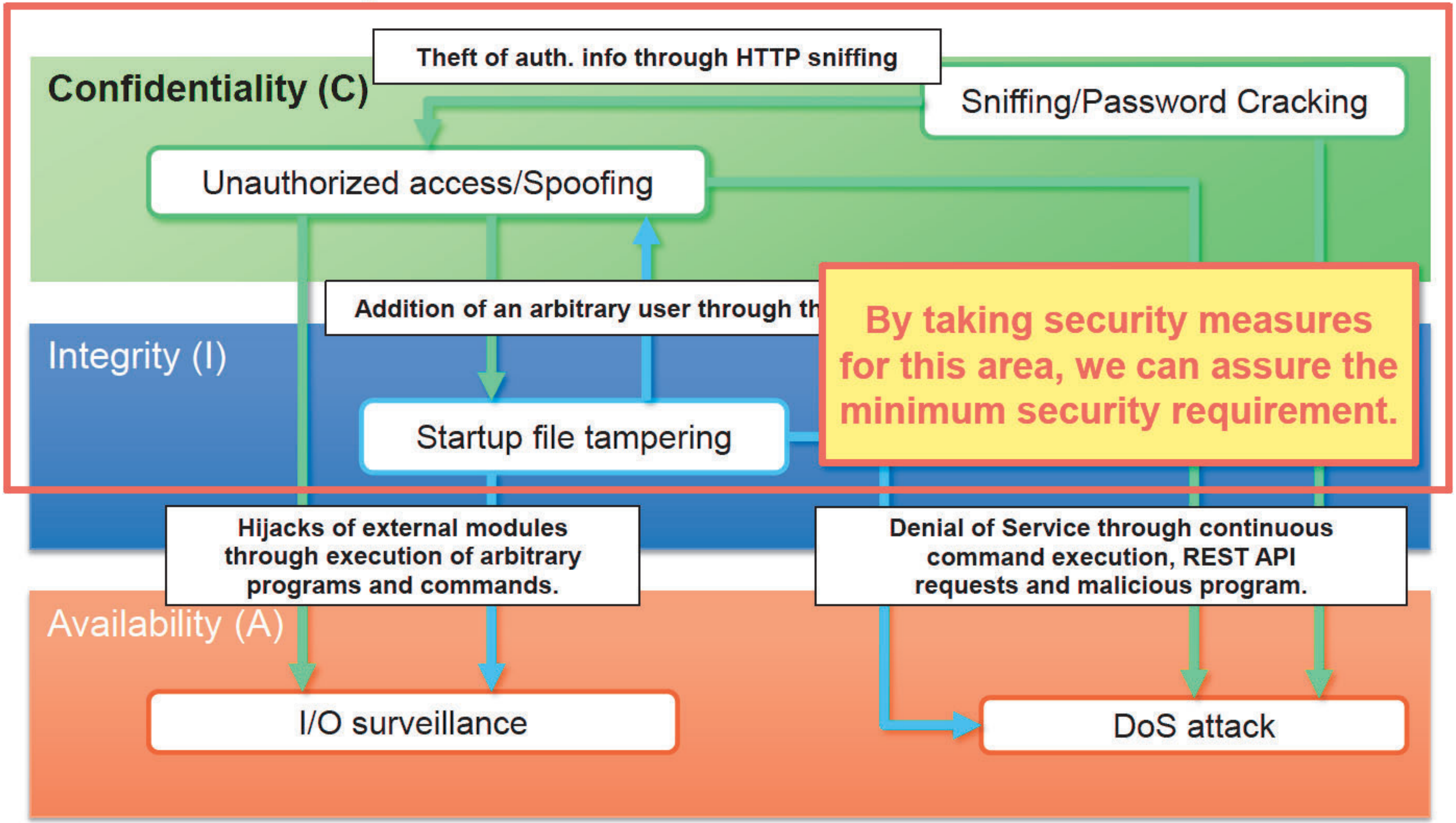
Password cracking through dictionary attacks and brute force just like for home routers.

Command execution, deployment of executables or backdoors by adding a new user exploiting FTP, SSH, remote debugging services.

Port scans and scanning of devices in the network through ICMP.

Recommended Security Measures for Windows 10 IoT Core

Relationships between Threats


Confidentiality (C)
Theft of auth. info through HTTP sniffing
Sniffing/Password Cracking
Unauthorized access/Spoofing
Integrity (I)
Addition of an arbitrary user through th
Startup file tampering
Hijacks of external modules through execution of arbitrary programs and commands.
Denial of Service through continuous command execution, REST API requests and malicious program.
Availability (A)
I/O surveillance
DoS attack

By taking security measures for this area, we can assure the minimum security requirement.

First thing to you should do after install

Unauthorized access/Spoofing

Sniffing/Password Cracking

- Change password
  - As a measure to prevent unauthorized access and spoofing, be sure to change the password of the built-in account through SSH or PowerShell.
  - The password should be complicated (strong enough) to prevent password cracks.

```
net user [username] [password]

To add a user:
net user [username] [password] /add
```

First thing to you should do after install (cont.)

Sniffing/Password Cracking

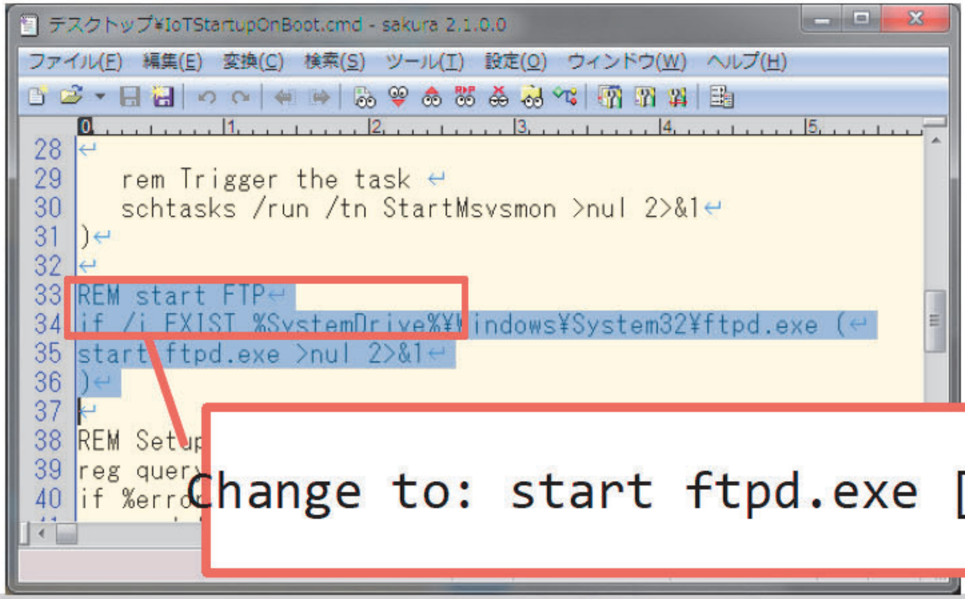
- Enable HTTPS
  - Configure HTTPS for the web UI as a measure to prevent a theft of authentication information by sniffing.
  - The configuration has to be done through the registry, so a reboot of the service or the device is required.

```
Reg add
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥IoT¥WebB /v
UseHttps /t REG_DWORD /d 1 /f
Reg add
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥IoT¥WebB /v
HttpsPort /t REG_DWORD /d <your port number> /f
```

Edit the startup file

Startup file tampering

- Disallow FTP from starting or change the root directory.
  - As a measure to prevent modification of IoTStartupOnBoot.cmd and other important files, remove the authentication-free FTP service from the startup file or change the root directory.



テスクトップ¥IoTStartupOnBoot.cmd - sakura 2.1.0.0
ファイル(F) 編集(E) 変換(C) 検索(S) ツール(T) 設定(O) ウィンドウ(W) ヘルプ(H)

```

    rem Trigger the task 
    schtasks /run /tn StartMsvsmon >nul 2>&1
)

REM start FTP
if /i EXIST %SystemDrive%¥Windows¥System32¥ftpd.exe (
start ftpd.exe >nul 2>&1
)

REM Setup
reg query
if %erro
```

```
Change to: start ftpd.exe [PATH_TO_DIRECTORY] >nul 2>&1
```

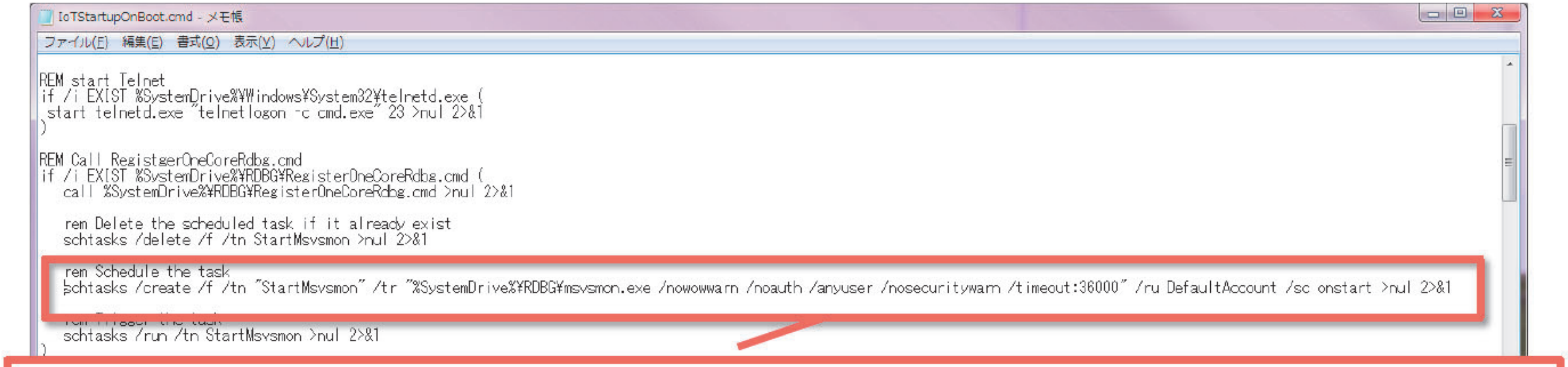
Edit the startup file (cont.)

Startup file tampering

I/O surveillance

DoS attack

- Enable authentication for remote debugging
  - Prevent unauthorized programs from being executed via the remote debugging service.


IoTStartupOnBoot.cmd - メモ帳
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

```
REM start Telnet
if /i EXIST %SystemDrive%¥Windows¥System32¥telnetd.exe (
 start telnetd.exe "telnetlogon -c cmd.exe" 23 >nul 2>&1
)

REM Call RegistgerOneCoreRdbg.cmd
if /i EXIST %SystemDrive%¥RDBG¥RegisterOneCoreRdbg.cmd (
   call %SystemDrive%¥RDBG¥RegisterOneCoreRdbg.cmd >nul 2>&1

   rem Delete the scheduled task if it already exist
   schtasks /delete /f /tn StartMsvsmon >nul 2>&1

   rem Schedule the task
   schtasks /create /f /tn "StartMsvsmon" /tr "%SystemDrive%¥RDBG¥msvsmon.exe /nowowwarn /noauth /anyuser /nosecuritywarn /timeout:36000" /ru DefaultAccount /sc onstart >nul 2>&1

   rem Trigger the task
   schtasks /run /tn StartMsvsmon >nul 2>&1
)
```

```
Change to: %SystemDrive%¥RDBG¥msvsmon.exe /timeout:36000“ /ru DefaultAccount /sc onstart >nul 2>&1
```

Configuration of Windows Firewall Rules

Unauthorized access/Spoofing

DoS attack

Probe by malware

- Customize Windows Firewall
  - Detailed configurations like inbound/outbound settings are available
  - Can also be written in the startup file
  - Example below is for blocking SSH connections

```
Check firewall status :
netsh advfirewall firewall show currentprofile

Block SSH(22) connection :
netsh advfirewall firewall add rule name=[RULE_NAME]
protocol=TCP localport=22 action=block

Check configuration :
Netsh advfirewall firewall show rule name=[RULE_NAME]
```

Summary

Have high expectation as a platform for IoT, but don’t consider it the same as the desktop version of Windows

- Unlike the desktop version of Windows, users are expected to configure the security as well, so it is unsafe to connect to the Internet with the default configuration.

- It is recommended to at least apply our security measures, however the configurations are complicated (especially Windows Firewall) and not much information are available compared to existing OS like Raspbian.

- Since Windows Update does not automatically apply security patches now, numerous devices may be left with known vulnerabilities unpatched in future.

Shouldn’t the platform assure the minimum security requirement?

- The FTP service and the remote debugging service should have authentication enabled by default and allow the user to select whether to keep it on or not.

- Some users of Raspberry Pi 2 use it for hobby and does not necessarily understand the risk of authentication-free FTP service and remote debugging service.

- Although IoT series belongs to the family of Embedded series, since it crowns the name of Windows and many uses can be expected with its free distribution, we believe that the platform should assure the minimum security requirement.

Thank you!

FFRI Inc.
http://www.ffri.jp