Open Sesame: Picking Locks with Cortana

Ron Marcovich, Yuval Ron, Amichai Shulman, Tal Be'ery
Amichai Shulman
- Independent Security Researcher
- Advisor for multiple cyber security start up companies
- Former CTO and Co-Founder of Imperva
- Blackhat, RSA, Infosec speaker
- @amichaishulman

Tal Be’ery
- Co-Founder @ Kzen Networks
- Formerly VP Research @Aorato (Acquired by Microsoft), Imperva, Singtel Innov8 VC
- Blackhat, RSA, SAS speaker
- @talbeerysec
Also Featuring...

Ron Marcovich
Twitter: @RonMarcovich
LinkedIn: ronmarcovich

Yuval Ron
Twitter: @RonYuval
LinkedIn: ronyuval

B.Sc. Software Engineering students at the Technion, Israel Institute of Technology. Both will start their M.Sc. In Computer Science this year.
• Understanding Cortana
  • What is it, how does it work and key elements

• Attacking Cortana on all fronts
  • Cortana agent: Open Sesame (CVE-2018-8140)
  • Cortana actions: The voice of Esau
  • Cortana cloud: Malicious skills

• Protecting against Cortana attacks
  • Voice Firewalls: NewSpeak

• Summary and Conclusions
Understanding Cortana
What is Cortana?

- "Your intelligent assistant across your life."
- Translate human intent into computer actions
  - Retrieve data
  - Browse the web
  - Launch programs
What is Cortana?

• Multi-platform: Mobile, PC, devices
• Multi inputs ("intents"): keyboard, mouse, voice, touch, ...
Cortana Architecture

Cortana Client

Cortana Service

Speech

Text

Resolve!

Card

Card data

Speech

Text

Intent + p

Intent to Card (Azure Bot)

Cortana Skill

Speech to Text

Text

Text to Intent (Action)

Intent + p

Intent to Card (Azure Bot)
• Very fat Client
  • Can do a lot of stuff!
  • Merely an execution engine
  • Exposes a powerful Javascript API
• Works on a locked devices
  • By Default!
  • SpeechRuntime.exe listens for “Hey Cortana”
  • SearchUI.exe has the “Cortana Logic”

Cortana uses more battery when this is on.
  
  - Respond when anyone says "Hey Cortana"
  - Try to respond only to me

Learn how I say "Hey Cortana"

Keyboard shortcut

Let Cortana listen for my commands when I press the Windows logo key + C
  
  - Off
  - On

Lock Screen

Use Cortana even when my device is locked
  
  - Off
  - On
• Processing and decision making is done in the cloud

• Two phases
  • Audio processing – Speech to Text
    • wss://websockets.platform.bing.com/ws/cu/v3
    • Binary + JSON
  • Semantic processing – Text to Intent & Intent to Card
    • https://www.bing.com/speech_render - GET request, HTML response
    • https://www.bing.com/DialogPolicy - GET / POST request, Javascript response

• Machine Learning
  • Improve speech recognition
  • Extend intent resolution capabilities
### Audio Processing Phase

#### Client vs. Server

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection.context(JSON)</td>
<td>IntermediateResult (XML)</td>
</tr>
<tr>
<td>Audio stream (BIN)</td>
<td>IntermediateResult (XML)</td>
</tr>
<tr>
<td>Audio stream (BIN)</td>
<td>PhraseResult (XML)</td>
</tr>
<tr>
<td>Audio stream (BIN)</td>
<td></td>
</tr>
<tr>
<td>Audio.stream.hypothesis</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Cortana can be extended with cloud based “skills”

• A Skill is an Azure bot registered to the Cortana channel

• Receive all user input after an invocation name

• Interacts with the Cortana client using Cards that include voice, text and LIMITED COMMANDS
Cortana Skills

Cortana’s Skill Framework overview

Build and Deploy
- Skill Source Code Written Using Bot Framework SDK
- Skill Deployment does not deploy ANY code to the client machine

Asynchronous “Activity” exchange via REST API
- Azure Bot sends Cortana’s server at Bing.com
- JSON response that describes the desired affect at the client’s machine

Enable Cortana Channel
- Invokes Skill and holds conversations

Cortana sends an HTML response with extensive use of JavaScript and CSS code with the desired actions
• Fat client executes on locked screen
• Many possible actions
• Action choice by cloud logic
  • Can be changed without any apparent sign on the device
  • Might depend on Machine Learning
• Choice of action can be affected by unknown 3rd parties

What can possibly go wrong?
“Anything that can go wrong will go wrong”

Edward A. Murphy, Jr.
Putting Murphy to Work

• Set up a research project with the Technion
• Undergraduate students exploring different aspects of the system
• Some avenues we explored
  • Local input to Cortana
  • Intents that invoke exploitable actions
  • Intents that retrieve malicious content
  • Capabilities of 3rd party Cortana skills
Attacking Cortana

- Local commands through lock screen
- Expressing bad intents
- Bad content provider
- Malicious skills

Cortana Service

- Speech to Text
- Text to Intent (Action)
- Intent to Card (Azure Bot)

Cortana Client

- Speech
- Text
- Resolve!

Card data

Internet

3rd party service

Speech

Text

Intent + p

Expressing bad intents

Malicious skills

Bad content provider
Open Sesame
CVE-2018-8140 (Open Sesame)

Grabbing Information
CVE-2018-8140 (Open Sesame)

Taking over
• Impact:
  • by Abusing The “Open Sesame” vulnerability, “Evil Maid” attackers can gain full control over a locked machine

• Evil Maid attack model:
  • Attackers have physical access for a limited time, but the Computer is locked

• Why it’s called Evil Maid?
  • Think of the laptop you left in your room last night when you went out...
  • But also borders control, computers in the office during breaks and night, ...

• But isn’t that exactly what Locked Screen suppose to stop?
• Lock Screen is not magic!
• Lock Screen is merely another “Desktop” (Winlogon desktop) with very limited access
• The security stems from the reduced attack surface
• If Microsoft adds more apps on Lock Screen: The attack surface expands → security is reduced
Lock Screen Evolution: Then
Lock Screen Evolution: Now
• Lock screen restricts keyboard, but allows Cortana invocation through voice
• Once Cortana is invoked, the Lock Screen no longer restricts it
  • Cortana is free to accept input from the keyboard too
• The fix: Make Cortana Search UI state aware. Different behavior when the UI is locked
• Shift of responsibility:
  • In the past, the OS made sure the UI is not accessible when computer is locked, therefore developers do not need to think about it.
  • Now, it’s the developers’ responsibility
Disclosure Timeline

16 APR 18:
We report CVE-2018-8140 to MS

12 JUN 18:
MS patch (Very quick + Bug Bounty!)

23 APR 18:
McAfee reports CVE-2018-8140 to MS

26 JUN 18:
We report CVE-2018-8369 to MS
• Impact: Evil Maid Attackers can gain full control on a locked machine
• The fix is
  • Tactical: making Cortana Search aware of UI state
  • Not Strategical: Cortana still gets keyboard input and launches processes from a locked screen in some other scenarios
• There are more where it came from: CVE-2018-8369
• Design lessons: Adding more capabilities to Lock Screen is very tempting, but dangerous
Cruel Intentions:  
The Voice of Esau
Attacking Cortana: Cruel Intentions

- Local commands through Lock Screen
- Expressing bad intents

Cortana Client → Cortana Service → 3rd party web service

Speech → Text to Intent (Action) → Intent to Card (Azure Bot) → Internet

Resolve! → Text → Intent + p → Card data

Cortana Skill

Intent to Card (Azure Bot)

Black Hat USA 2018
Voice of Esau Attack

- Evil Maid Attack (First presented in Kaspersky SAS 2018)
- Attackers:
  1. Achieve Man-in-the-Middle position: Plug into the network interface
  2. Use Cortana on locked screen to invoke insecure (Non-HTTPS) browsing
  3. Intercept request, respond with malicious payload
     - Exploit browser vulnerabilities
     - Capture domain credentials
The VOE Attack - Evil Maid (Local)

I'm in! but the computer is locked!

Hi Cortana!
Go to bbc.com

I'm BBC and here's my malicious payload!

Browse http://www.bbc.com
The VOE Attack Demo
• Use initial compromise to install agent on compromised machine
• Achieve Man-in-the-Middle position
  • Some local routing attack: e.g. ARP spoofing
• Invoke Cortana insecure browsing
  • Play sound file – “GOTO BBC DOT COM”
  • RDP (Remote Desktop Protocol) sound file to target
    • NLA must be disabled for it to work
• Intercept traffic of targeted machines and compromise, as in before.
RDP: A Silent Killer

Silent Killer Diseases
You Must Know

Connect to win10-cortana-vuln

Audio Settings

Remote audio playback
- Play on this computer
- Do not play
- Play on remote computer

Local devices and resources
- Printers
- Clipboard

Remote audio recording
- Record from this computer
- Do not record

Connect | Help
Cortana over RDP Demo
16 JUN 17: We report VOE to MS

29 JUN 17: MS Cloud patch (no CVE)

8 MAR 18: Our talk @ Kaspersky SAS

25 JUN 18: We report CVE-2018-8271 (and more) to MS
The Voice of Esau

- Impact: Evil Maid or even remote attacker can invoke unsafe browsing on a locked machine. Using additional vulns attacker can gain full control.

- The fix is
  - Tactical: making Cortana cloud aware of UI state and safely Bing instead of direct browse in certain scenarios
  - Not Strategical: Cortana may still allow unsafe browsing in some other scenarios

- There are more where it came from: CVE-2018-8271 (and more)

- Design lessons: Adding more capabilities to Lock Screen is tempting but dangerous
Skill of Death
• VOE attack took advantage of existing intent resolution mechanisms
• What about adding our own interpretation mechanism?
• Skills interact with client through cards
• Cards have “limited functionality”
Navigate to an attacker controlled server

Open malicious MS Office document
Skill of Death
• How can attacker invoke a “malicious” skill?
  • Invoking a new skill on a machine requires user consent
• Cortana Skill can be invoked and granted consent from locked screen!
Skill of Death

• Timeline
  • Authorization of skills in locked screen detected March 2018
    • Guy Feferman and Afik Friedberg of The Technion, Israel
  • Takeover methods detected June 2018
    • Natanela Brod and Matan Pugach of the Technion, Israel

• Fixed on June 25th 2018
  • Fixed in the cloud
    • No formal announcement of fix
    • Skills can no longer be INVOKED (authorized or not) from locked screen

• Adding functionality on locked screen is a slippery slope
  • Soon you find yourself allowing NON Microsoft code to run over locked screen
Protection
Preventing Voice Attacks: Speaker Identification

• Respond only to me
• “try” doesn’t sound very reassuring
• “Hey Cortana” can be easily recorded
• Can be subverted, see other talk
Preventing Voice Attacks: Compensating Controls Take 1

- Take 1: Put a security Microphone on each room?

- Disadvantages:
  - Privacy
  - Cost
  - Audio directionality
  - Audio semantics
  - Not all attacks are audible
  - Detection only
• NewSpeak: a Network-based Intercepting proxy
• TLS/SSL certificate must be installed on monitored devices
  • In many organizations already exists for web gateway monitoring, DLP
• Can monitor all Cortana requests and responses
  • Origin details: IP, computer name, user, UI State, etc.
  • Request audio and Text to Speech results
  • Intents and Action cards
• Can block or modify all Cortana requests and responses
• Much better than previous suggestion: Centrally located, does not rely on audio analogic capture, can mitigate not just detect
Hi Cortana!
Go to cnn.com

Browse http://www.cnn.com

Browse http://www.foxnews.com

I’m the NewSpeak Proxy

Network monitoring with NewSpeak
Summing up
Summary: Attacking Cortana

- Local commands through Lock Screen
- Expressing bad intents
- Malicious skills
- Bad content provider

Cortana Client → Cortana Service

- Speech
- Text
- Resolve!
- Card data

Cortana Service → Internet

- Speech to Text
- Text to Intent (Action)
- Intent to Card (Azure Bot)

Internet → 3rd party service

Card data → Intent to Card (Azure Bot)

Expressing bad intents

Malicious skills

Bad content provider
• For the time being:
  • Disable Cortana voice in corporate environments
  • Or at least on locked screen
• Reconsider when compensating controls are there
• “voice firewall”: If voice becomes mainstream, considering specialized solutions is a must for corporate adoption

https://www.pcgamer.com/how-to-disable-cortana/
• New interfaces are much more than “just an interface”
• When introducing innovative concept into existing environments
  • Secure Coding is not enough
  • We need Secure System Engineering
• We found 3 different CVEs and numerous issues that enables attackers to bypass the lock screen
Questions?