Open Sesame: Picking Locks with Cortana

January 24, 2019
Speakers

Featured Presenter:

Amichai Shulman,
Cyber security researcher, entrepreneur and investor

Sponsor Presenter:

Deral Heiland,
IoT Research Lead,
Rapid7
• Tal Be’ery of Kzen Networks

• From the Technion – Israeli Institute of Technology
  • Prof. Eli Biham
  • Yuval Ron
  • Ron Marcovich
  • Natanela Brod
  • Matach Pugach
  • Guy Feferman
  • Afik Friedberg
  • Liraz Keinan
  • Or Yasu
Cortana Architecture
Cortana Architecture - Example

Cortana Client

Speech

Who is George Washington

Resolve!

Cortana Service

Speech

Who is George Washington

Text to Intent (Action)

Search
Query = “George Washington”

Search
Query = “George Washington”

Intent to Card (Azure Bot)

Card data

Internet

3rd party web service
Cortana Agent

- 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

Lock Screen
Use Cortana even when my device is locked
- On
Cortana Cloud Service

• 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
Semantic Processing Phase
Cortana Skills

• 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
Summary

• Fat client executes on locked screen
• Many possible actions
• Action choice by cloud logic
  • Can be changed without any apparent sign
  • Might depend on Machine Learning
• Choice of action can be affected by unknown 3rd parties
“Anything that can go wrong will go wrong”

Edward A. Murphy, Jr.
Attacking Cortana

Local commands through lock screen

Expressing bad intents

Malicious skills

Bad content provider

Cortana Client → Speech → Cortana Service

Cortana Service → Text to Intent (Action) → Intent to Card (Azure Bot)

Card data → Card Action Provider

Internet → 3rd party service

Resolve!

Speech to Text

Card

Intent + p

Intent + p
Local Attacks

Open Sesame and More
CVE-2018-8140 (Open Sesame)
Open Sesame: Attack Model

• 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

• But isn’t that exactly what Locked Screen suppose to stop?
Lock Screen: You Had One Job

- 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
- Responsibility for security is shifted to individual application programmers
Hey Cortana, Remind Me to Take Over

• Invoke the “Reminder” skill
  • “Hey Cortana set up a reminder”
• You can attach a photo to a reminder (why???)
• Invokes a file chose dialog
• The equivalent of DOS command line
Hey Cortana, Call 1-800-HACKME

- Ask Cortana do display a phone number
  - “Hey Cortana, what is my phone number”? 
  - “Hey Cortana, what is the phone number of Microsoft customer support”
- MS Edge converts phone numbers in display to special links
- Invokes the “People” app
- Add contact
  - Add a photo of your contact...
Cruel Intentions
The Voice of Esau
Voice of Esau Attack

• Evil Maid Attack (First presented in Kaspersky SAS 2018)
• Attack walkthrough
  • Achieve Man-in-the-Middle position: Plug into the network interface
  • Use Cortana on locked screen to invoke insecure (Non-HTTPS) browsing
  • Intercept request, respond with malicious payload
    • Exploit browser vulnerabilities
    • Capture domain credentials
• “Fixed” – August 2017
The VOE Attack - Evil Maid (Local)

Hi Cortana!

Go to bbc.com

Browse http://www.bbc.com

I’m BBC and here’s my malicious payload!
The Voice of Esau Returns!
The Voice of Esau Returns!

• There are many ways to say please 😊
• Multiple additional sentences are interpreted as “take me to some domain”
  • Go to BBC
  • Launch BBC
• Using machine learning, Cortana circumvented the patch!

• Reported to MS in June 2018
• Fixed September 2018
• Re-introduced October 2018
• Annihilated November 2018
The Revenge of the Voice of Esau
The Revenge of the Voice of Esau

• Cortana’s built-in services generate cards with non-SSL links in them
• Clicking the link invokes non-SSL browsing in the background
• Much easier to exploit
  • MITM attack can be invoked after Cortana communications are finished
  • Timing of MITM is easier to control
The Voice of Esau European Vacation
The Voice of Esau European Vacation

- Cortana’s built-in mechanisms construct cards with links to attacker controlled servers
- Clicking the link invokes browsing, in the background to the attacker controlled server
- No MITM attack is required!
- Attacker needs to figure out how to promote the web server
  - Enough web presence
  - Popular blog
  - (Dead) Wikipedia entry
- CVE-2018-8253
Skill of Death
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”
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

21:10
Monday, March 12
Skill of Death – Limited Functionality

Navigate to an attacker controlled server

Open malicious MS Office document
Skill of Death
This is where we show that a skill can open Word document from the web

Amichai Shulman, 02/07/2018
Summary

• When adding new interactive concepts
  • Revisit your security assumptions
  • Don’t assume secure + secure = secure
  • Test for new attacks not the old ones
• Adding functionality to locked screen is a slippery slope

• By November 2019 MS effectively blocked any Cortana functionality over locked screen
• Our continuous research shows that this can be bypassed as well
• We found similar vulnerabilities with Siri, Bixby and Cortana for Android
Questions & Answers

Featured Presenter:
Amichai Shulman,
Cyber security researcher, entrepreneur and investor

Sponsor Presenter:
Deral Heiland,
IoT Research Lead,
Rapid7

• To join the Black Hat mailing list, email BH LIST to:
  feedback@blackhat.com

• To join our LinkedIn Group:
  http://www.linkedin.com/groups?gid=37 658&trk=hb_side_g

• To follow Black Hat on Twitter:
  https://twitter.com/Blackhatevents

• Black Hat’s Facebook Fan Page:
  http://www.facebook.com/blackhat

• Find out more at www.blackhat.com

• Next Webcast: February 21, 2019
Thank You!

@BlackHatEvents / #BlackHatWebcasts