YOU SHOULD BE able to trust your wireless keyboard. And yet security researchers have been warning people to be suspicious of wireless computer accessories using sketchy radio protocols for years. Those warnings peaked five months ago, when hackers at the security firm Bastille found that millions of cheap keyboard and mouse dongles let hackers inject keystrokes onto your machine from hundreds of yards away. Now, in case you missed that message, the same researchers have extended their attack to millions more devices—and this time, they can not only inject keystrokes, but also read yours, too.
who are we?

Kevin Chan : Team Lead
4th Year Computer Engineering

Albert Chen
4th Year Computer Engineering

Trevor Morris : Team Scribe
4th Year Computer Engineering

Robert Stosick
4th Year Computer Engineering

Henry Yu
3rd Year Computer Science

Renato Untalan
Novacoast, UCSB CS '09
bluetooth 4.0

bluetooth le/smart
- subset of bt 4.0
- uses lower power radio frequency
- always on
- iphone 5 and later
- fitbits, medical devices, remotes
> 90% of smartphones will be bluetooth smart ready by 2017
problem: security flaws

vulnerabilities:
>- confidentiality
>- integrity
>- availability

range is larger than you think:
>- 100m or 328 ft
man-in-the-middle

general

Alice  Eve  Bob

bluetooth

Phone: "Alice"

Device: "Eve"

Bluetooth Headset: "Bob"
novatooth
a pen-testing platform

increase awareness + exposure

Eavesdrop

WinRecon

BluePhish
eavesdrop
a passive MiTM implementation

Phone “Alice”

NovaTooth “Eve”

Web Backend

Google Cloud Speech

Bluetooth Headset “Bob”

no integrity!
bluephish
an active MiTM implementation

Phone “Alice”

NovaTooth “Eve”

Web Backend

Google Cloud Speech

Bluetooth Headset “Bob”

no integrity!
steps

scan  3 way handshake  phone call
recording audio

Recording MP3 files:
- Mon Feb 27 14:36:39 UTC 2017. mp3
- Mon Feb 27 15:56:42 UTC 2017. mp3
- Mon Feb 27 15:57:20 UTC 2017. mp3

pulseaudio
winrecon
a distributed bt surveillance grid

- windows-based bt spyware
- loaded on flash drives
- creates a botnet of infected computers
- infected computers scan for nearby bt devices
winrecon
a distributed bt surveillance grid

- track devices as they move between nodes
- scan for outdated devices
- track the # of visitors per hour in a given area
backend

- Eavesdrop
- WinRecon
- BluePhish

 Technologies:
- AWS
- Django
- Google

next >
DEMONSTRATION
development practices
DEMONSTRATION
Thank You!