RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: MBS-W04

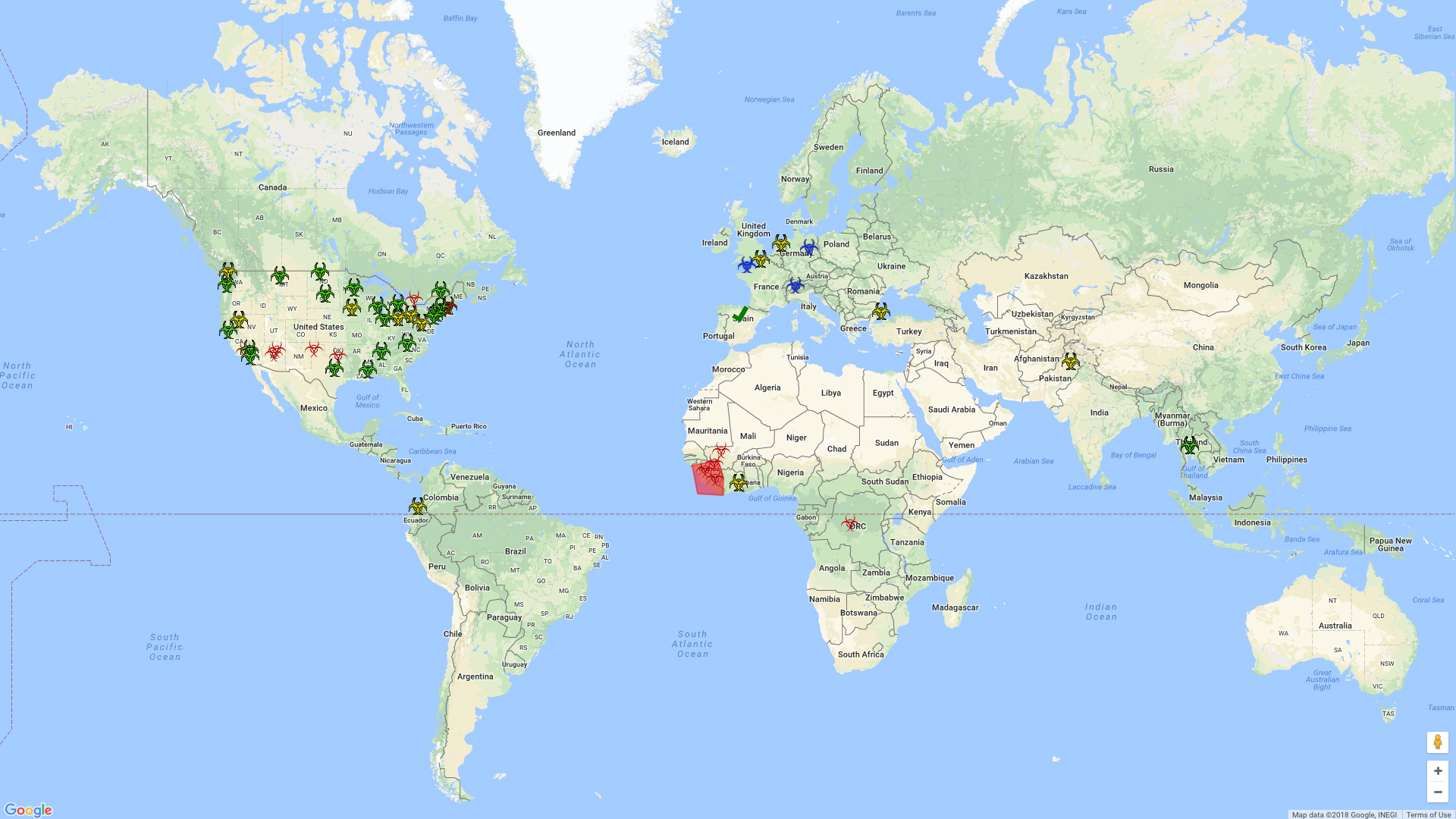
THE NEW LANDSCAPE OF AIRBORNE CYBERATTACKS

Nadir Izrael

CTO & Co-Founder
Armis, Inc.

Ben Seri

Head of Research
Armis, Inc.


Baffin Bay
Barents Sea
Kara Sea
East Siberian Sea
Norwegian Sea
Greenland
Iceland
Northwestern Passages
Hudson Bay
Canada
United States
Mexico
Gulf of Mexico
Cuba
Puerto Rico
Caribbean Sea
Guatemala
Nicaragua
Venezuela
Guyana
Suriname
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Argentina
Uruguay
North Pacific Ocean
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Sweden
Finland
Norway
Russia
United Kingdom
Ireland
Denmark
Germany
Poland
Belarus
Ukraine
France
Austria
Romania
Italy
Spain
Portugal
Greece
Turkey
Kazakhstan
Mongolia
Uzbekistan
Kyrgyzstan
Turkmenistan
China
South Korea
Japan
Sea of Okhotsk
Sea of Japan
East China Sea
Afghanistan
Iran
Iraq
Syria
Pakistan
Nepal
India
Myanmar (Burma)
Thailand
Vietnam
Philippines
Philippine Sea
South China Sea
Bay of Bengal
Arabian Sea
Laccadive Sea
Gulf of Aden
Gulf of Thailand
Malaysia
Indonesia
Banda Sea
Arafura Sea
Papua New Guinea
Coral Sea
Tasman
Australia
Great Australian Bight
Tanzania
Kenya
Somalia
Ethiopia
South Sudan
Sudan
Yemen
Oman
Saudi Arabia
Egypt
Libya
Algeria
Tunisia
Morocco
Western Sahara
Mauritania
Mali
Niger
Chad
Nigeria
Burkina Faso
Ghana
Gulf of Guinea
Gabon
DRC
Angola
Zambia
Mozambique
Zimbabwe
Namibia
Botswana
South Africa
Madagascar
Map data ©2018 Google, INEGI
Terms of Use


NOTHING SPREADS LIKE FEAR
CONTAGION
armis
participant MEDIA
imagenation abu dhabi
RSAConference2018
WARNER BROS. PICTURES
©2011 Warner Bros. Ent. All Rights Reserved

THE NEW ATTACK LANDSCAPE

The Airborne Attack

armis

RSAConference2018

The Airborne Attack

BROADPWN

BlueBorne™

Key Reinstallation Attack

GOOGLE PROJECT ZERO

RCE on Broadcom Wifi FW

No User Interaction Required

Internet

URL Link

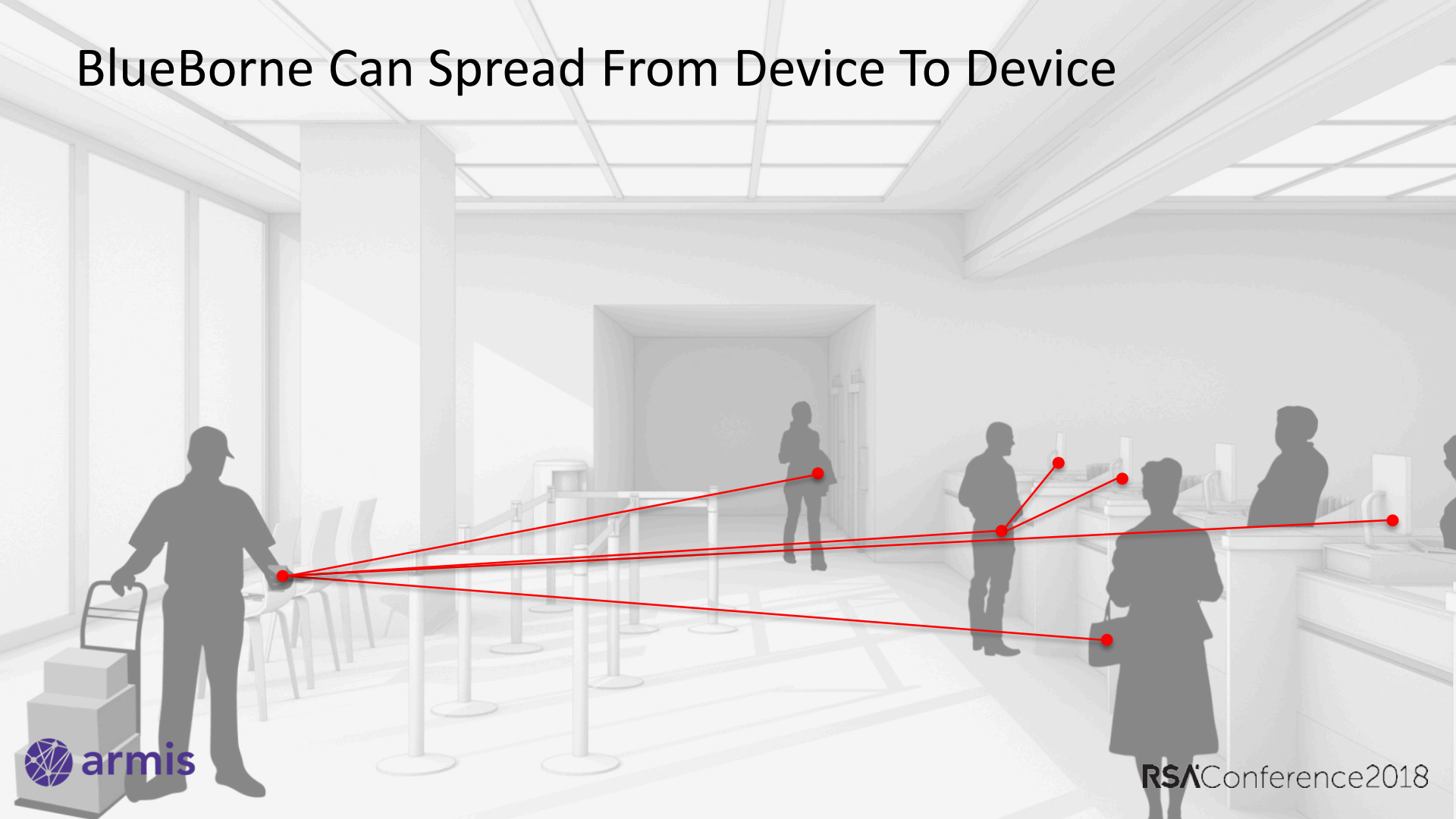
Download

Pair Device

“Bluetooth’s Stagefright Moment”

- 5.3B+ Devices At Risk
- 2B+ Unpatchable
- 9 Zero-Day Vulnerabilities (4 critical)
- Android, Windows, Linux, and iOS
- Most serious Bluetooth vulnerability to date
- Enables RCE and MiTM

BlueBorne Can Spread From Device To Device



armis

RSAConference2018

armis

RSAConference2018

What Systems Are Impacted

Google	Microsoft			amazon
✓ Patches Available	✓ Patches Available	✓ Patches Available	✓ Mitigated iOS 10+	✓ Patches Available

• 1 Info Leak
• 2 RCE
• 1 MiTM
	• 1 MiTM	• 1 Info Leak
		• 1 RCE
			• 1 RCE
			  • Pre-iOS 10
			  • Pre- tvOS 9
				• 1 Info Leak
				• 1 RCE

• Google Pixel • Samsung Galaxy • Samsung Galaxy Tab • LG Watch Sport • Google Home	• Windows Desktops • Windows Laptops	• Samsung Gear S3 (Smartwatch) • Samsung Smart TVs • Samsung Family Hub (Smart refrigerator)	• iPhone • iPad • iPod • Apple TVc	• Amazon Echo

armis

armis

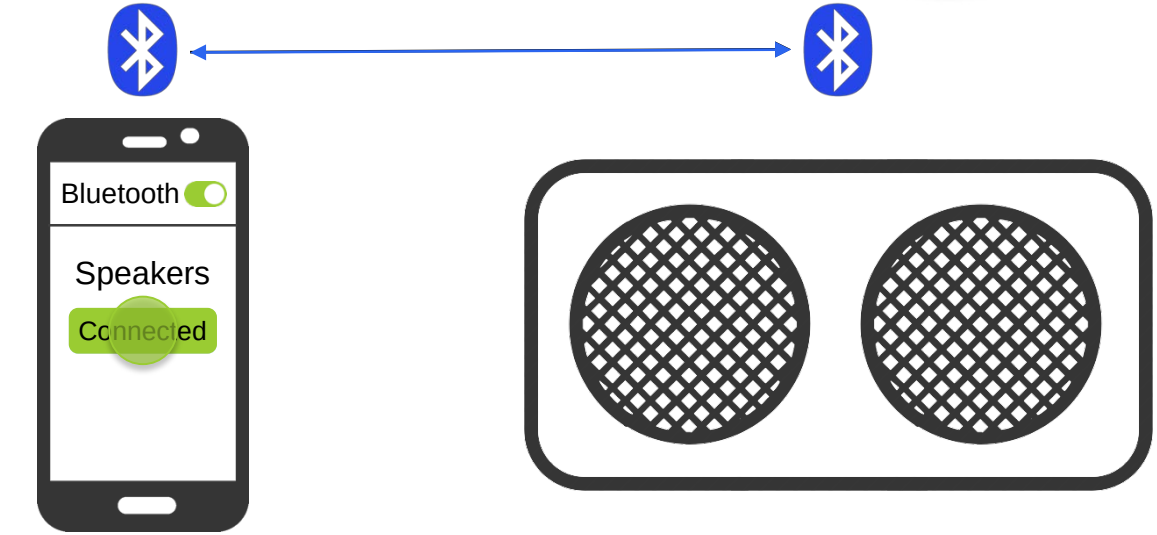
RSAConference2018

How BlueBorne Works

High Privileges

How BlueTooth Pairs

- Bluetooth is “on” and discoverable
- User must find and proactively “pair” to the device
- Some authentication or PIN to connect
- Devices exchange keys, and auto connect without discoverable mode



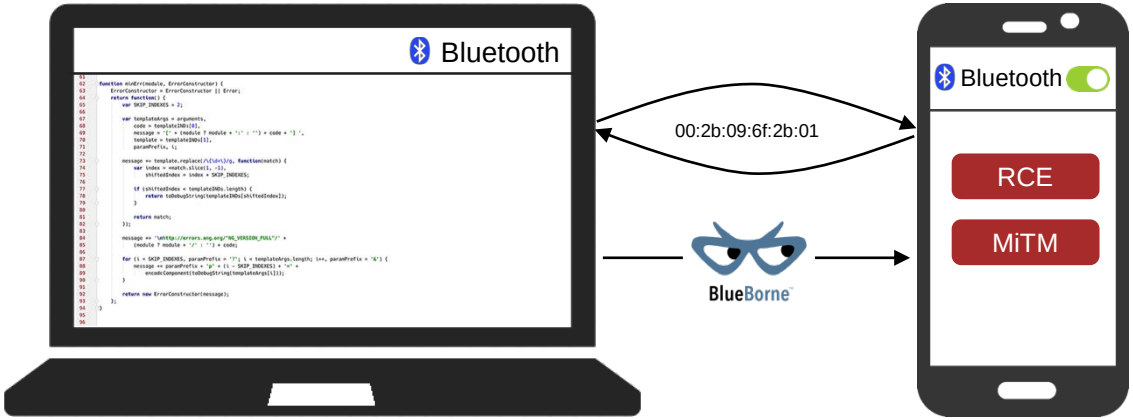
Device 1
(Smart Phone)

Device 2
(Bluetooth Speakers)

armis

How BlueBorne Works

- Bluetooth is “on”
- Attacker gets the MAC address
- Attacker initiates Bluetooth and attacks via using a BlueBorne vulnerability
- No user interaction required
  - No pairing
  - No approval
- Attacker can take over, create MiTM, get encryption keys, etc.



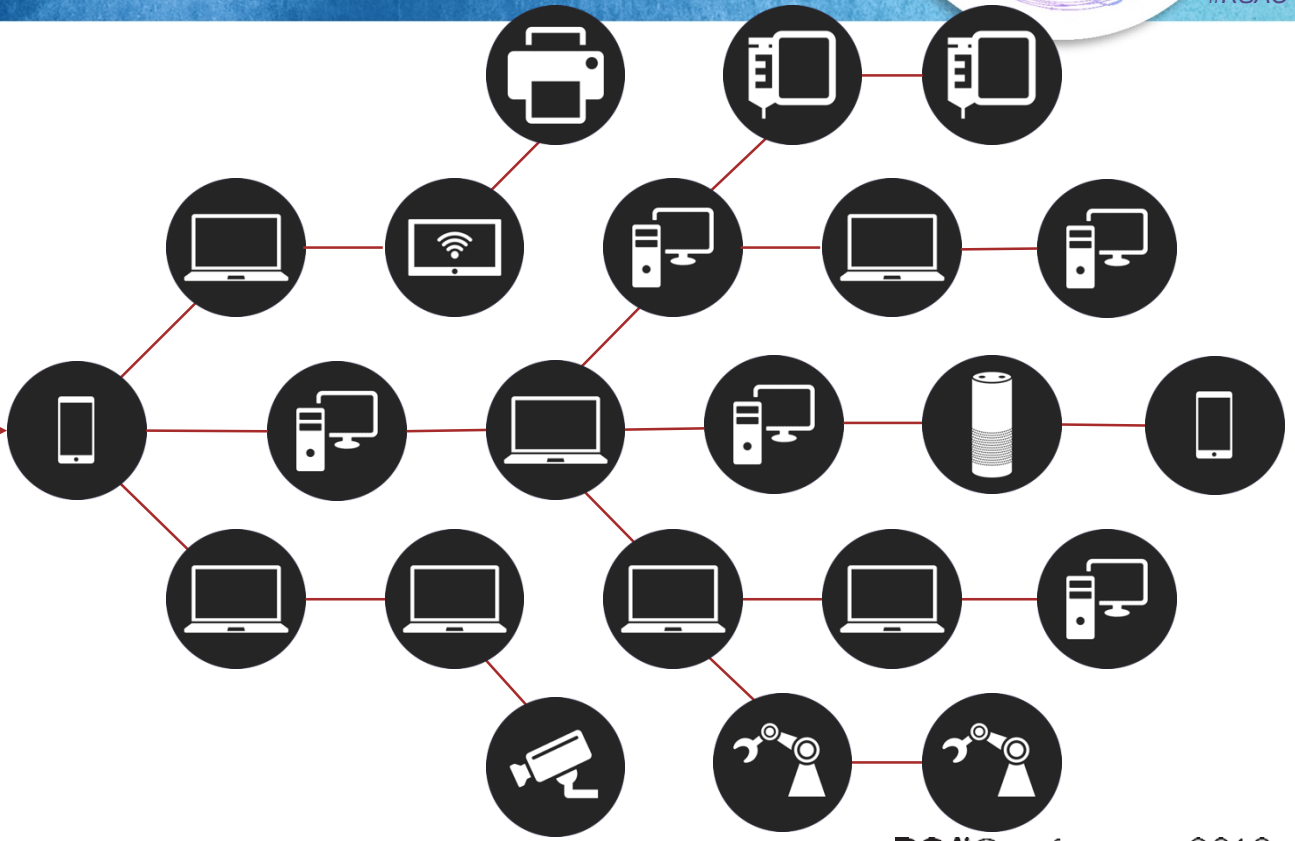
Attacker
(Laptop)

Target
(Smart Phone)

A BlueBorne Worm

Attacker

- Worm-like potential
- Deliver ransomware
- Spread botnet
- Steal credentials
- More…

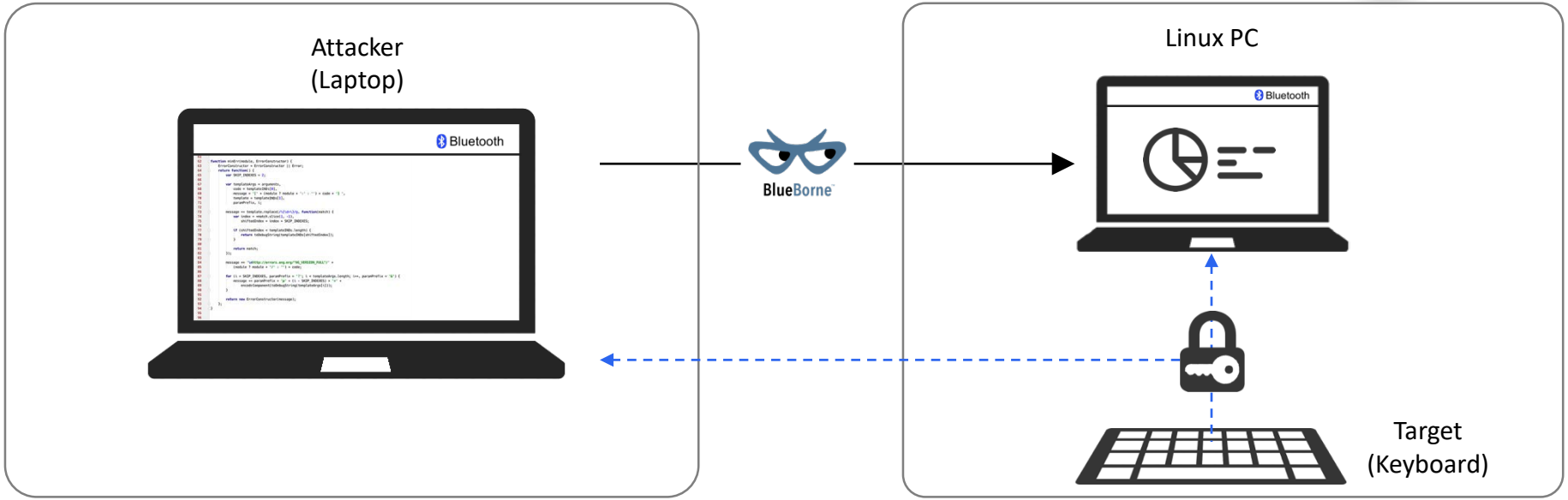


armis

BlueBorne™

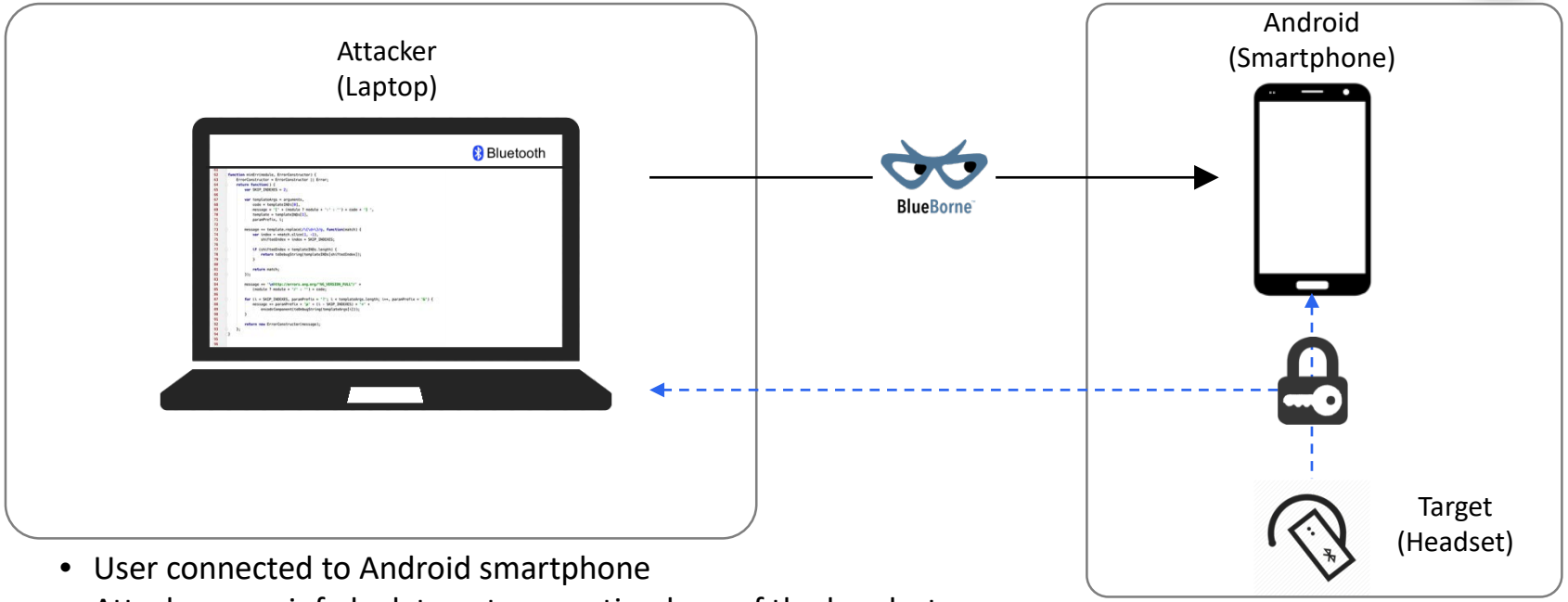
Info Leak

Info Leak (To Desktop)



- User connected to Linux desktop Attacker uses info leak to get encryption keys of the keyboard
- Attacker intercepts keystrokes without running code or doing MiTM
- Attacker can also inject keystrokes to the targeted device

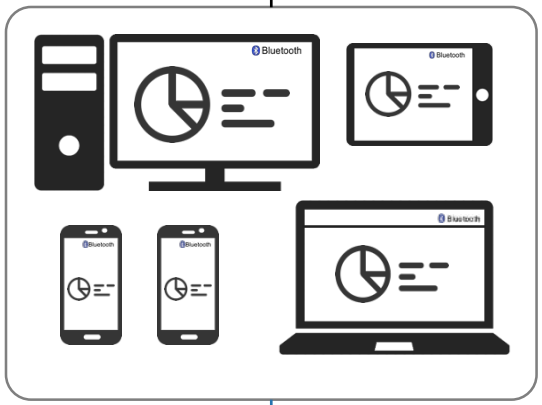
Info Leak (Headset)



- User connected to Android smartphone
- Attacker uses info leak to get encryption keys of the headset
- Attacker intercepts headset audio (eavesdropping on calls for instance)

Man in the Middle Attack

MiTM – WiFi Pineapple



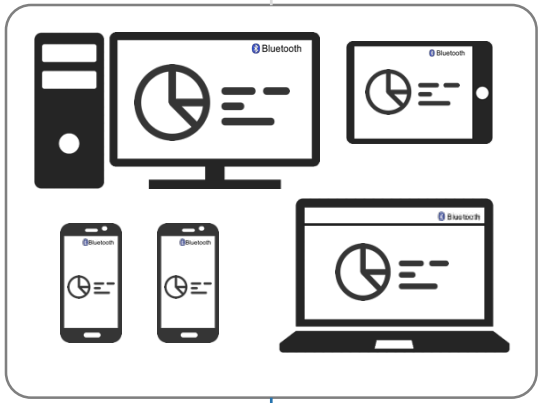
Corporate Network

Internet

IMPORTANT
User Interaction Required – Users Select The Network

WiFi Pineapple

MiTM – Bluetooth Pineapple



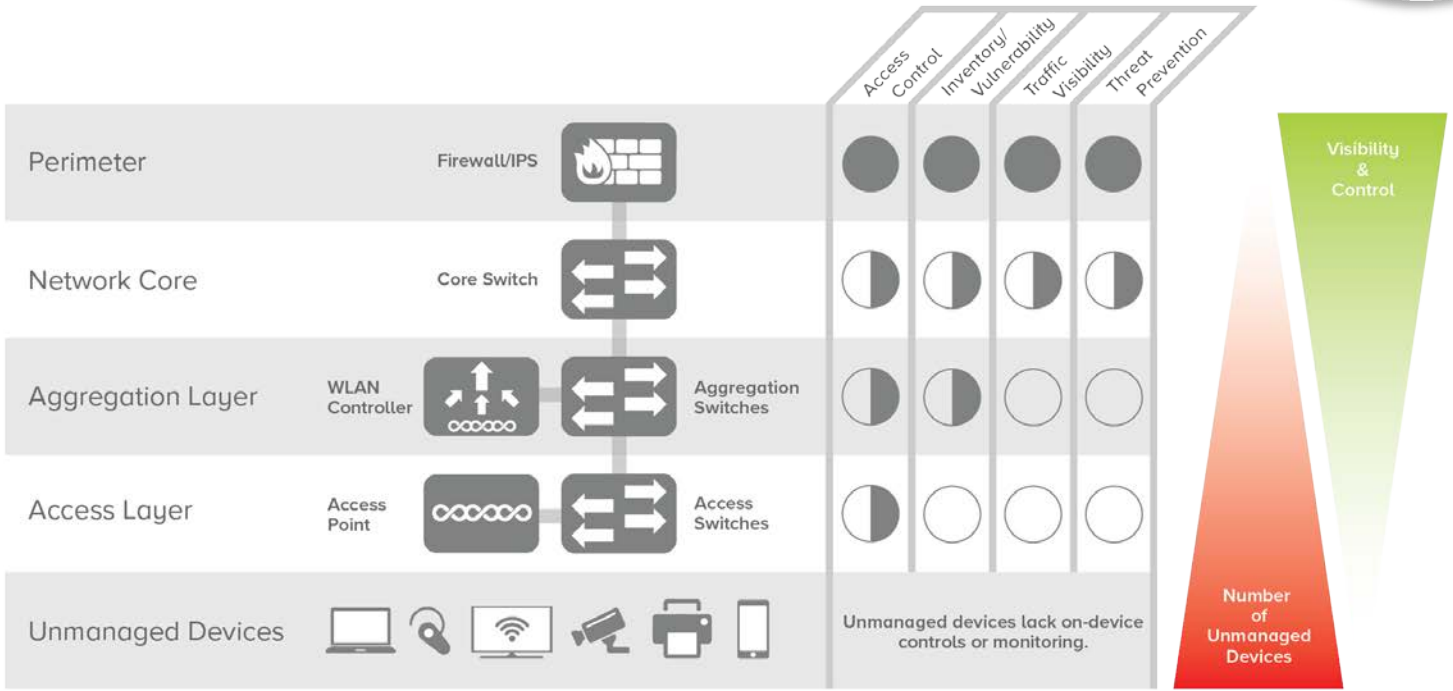
Corporate Network

Internet

IMPORTANT
No User Interaction Required

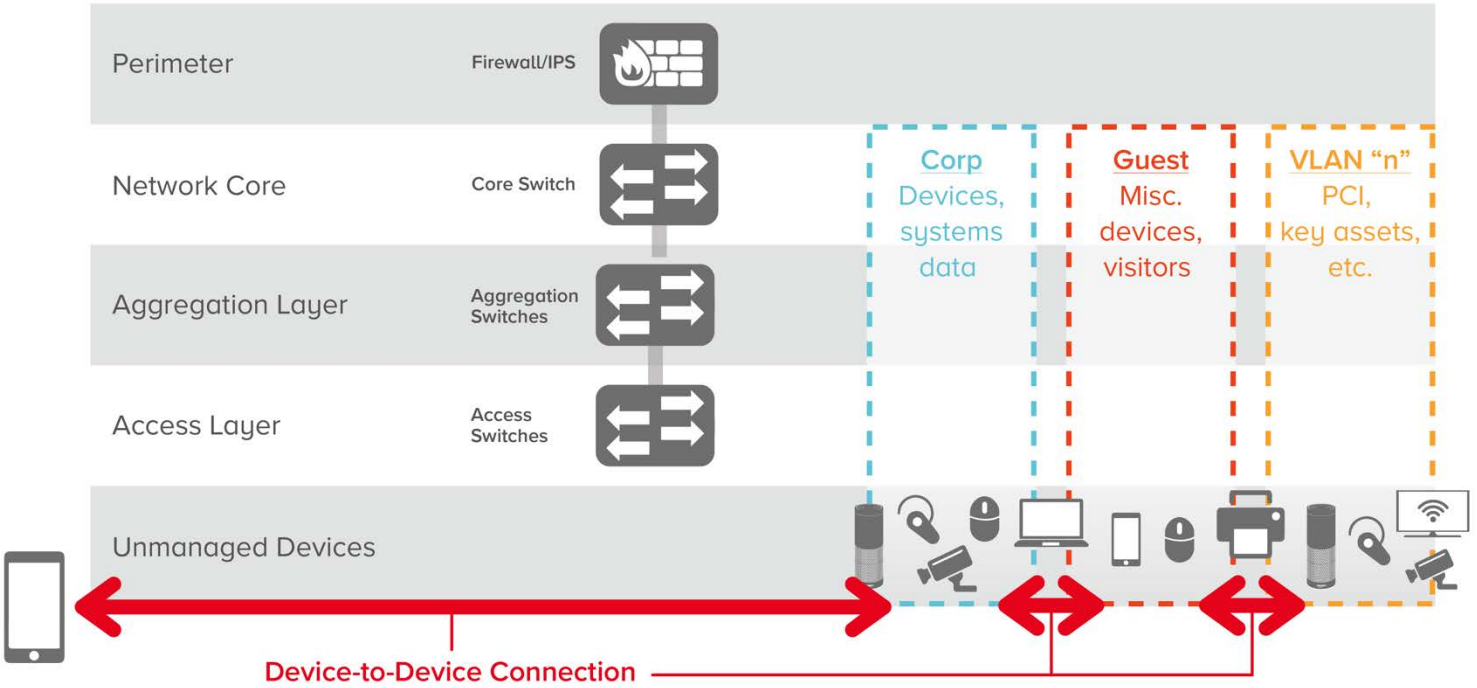
Bluetooth Pineapple

The Challenge Facing Us



Visibility and control is the least where unmanaged device density is the greatest.

Air Gap'ing Will Not Protect Us



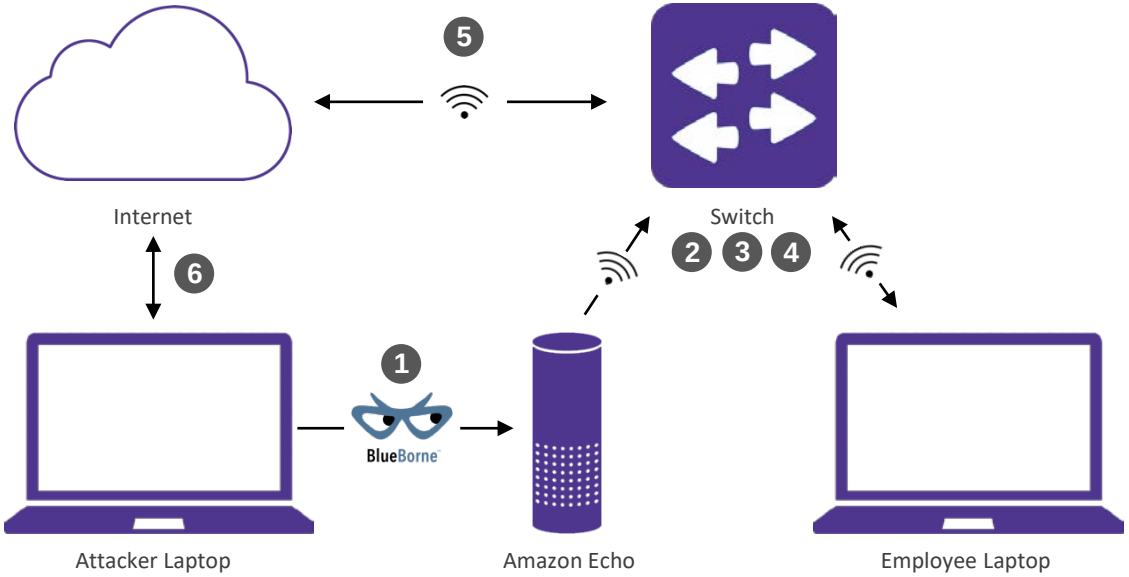
DEMONSTRATION

BlueBorne Attack

armis

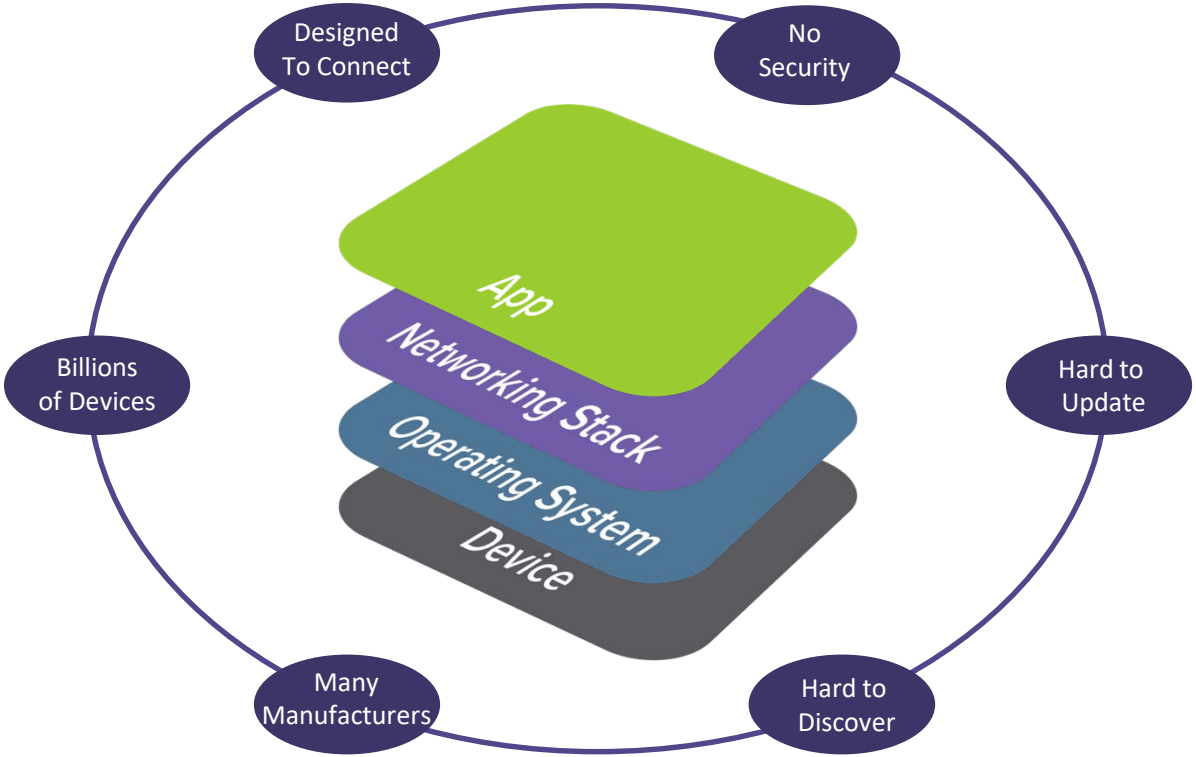
RSAConference2018

BlueBorne Attack



1. IoT device attacked
   - Amazon Echo taken over via BlueBorne
2. Echo controlled via Internet
   - Attacker switches control of Echo via Internet
3. Switch is compromised
   - Via the Echo, attacker compromises the Switch
   - Gains access to all connected devices via “low level” exposure
4. Confidential data accessed
   - Attacker captures critical data
   - Passwords, credentials, etc.
5. Data passed via Internet
   - Bluetooth no longer used
   - Amazon Echo no longer used
6. Hacker gets data
   - Obtains critical information
   - Can continue to infiltrate or exfiltrate

Meet the New Endpoint



armis

IMPLICATIONS AND NEXT STEPS

armis

RSAConference2018

The Implications

- Researcher – More is needed
- Manufacturers – Provide simple method to update
- Developers – Check for latest versions
- Security Professionals – Proactively seek out these devices
- Businesses – Have policies and protocols

Recommendations

Device and network discovery and visibility are critical.

Next Steps

	Immediately	Month 1	Month 3	Month 6+
Discovery	Discovery Report Critical Exposures New Acquisitions			
Cross Team Meeting		Cross Functional Meeting (Security, Networking, Operations, Facilities)		
Identify Program			Policies Employee Education Rapid Response Identify Solution	
Implement Program				Implement

QUESTIONS