MARIST

School of Computer Science and Mathematics

Cybersecurity for the Internet of Things: Vulnerabilities of a Smart Doorbell System

Claudia Rojas and Casimer DeCusatis, Ph.D. casimer.decusatis@marist.edu

NY State Cloud Computing & Analytic Center, Marist College

Overview

- Cybersecurity at Marist College
- Background
- Experimental Setup
- Results
- Summary & Future Research Directions

MARIST

School of Computer Science and Mathematics

Cybersecurity at Marist College

- B.S. degree in Cybersecurity
  - Hacking & Penetration Testing
  - Mobile Security
  - Computer Forensics & Ethical Hacking
    https://www.marist.edu/computer-science-math/cybersecurity
- Minor in Cybersecurity
- Education & Research SOC
  https://patch.com/new-york/midhudsonvalley/marist-opens-center-cybersecurity-program
- Online IDCP Certification from NY State
  http://idcp.marist.edu/enterprisesystemseducation/cybersecurity.html
- Summer high school program for college credit
  http://ww2.marist.edu/summerinstitutes/cybersecurity/
- Marist Innovation Lab on GitHub
  https://github.com/Marist-Innovation-Lab

SECTIONS THE CHRONICLE OF HIGHER EDUCATION LOG IN

SUBSCRIBE TODAY

SPECIAL REPORTS

Innovations in Cybersecurity Benefit Graduates and the Nation

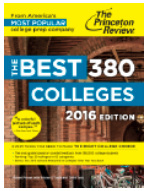
By Paul Basken | FEBRUARY 26, 2017 PREMIUM CONTENT FOR SUBSCRIBERS. SUBSCRIBE TODAY

Universities that have an expansive sense of cybersecurity, offering programs that go beyond just teaching code, may be better positioned to help their graduates find jobs and help the country thwart costly or deadly attacks. Following are some of...

Cybersecurity job posting grew 114% from 2011 to 2015, with 86% requiring at least a B.S. degree.
4 year colleges are meeting only about 24% of this demand.

- Cybersecurity Program High Level Overview:
  - Based on NIST Risk Management Framework
  - Labs cover ISC^2 certification requirements
  - Covers all topics requires for U.S. Government courseware certification NSTISSI 4011: National Training Standard for Information Systems Security (INFOSEC) Professionals http://en.wikipedia.org/wiki/Committee_on_National_Security_Systems
  - Publisher provides a mapping to requirements from the following organizations:
    - National Centers of Academic Excellence (CAE)/Cyber Defense Education Program
      NSA/DHS sponsored program through CISSE http://www.cisse.info/
    - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
      http://csrc.nist.gov/nice/framework/
      and the DHS National Initiative for Cybersecurity Careers and Studies (NICSS)
      http://niccs.us-cert.gov/
    - Department of Defense Cybersecurity Workforce Strategy (DCWS) and Workforce Development Framework (CWDF)
      including DoDD 8570.01 Information Assurance Training, Certification and Workforce Management (emerging)
      http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed%28final%29.pdf

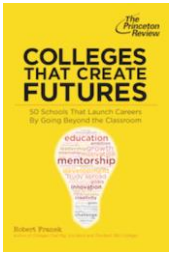
BEST U.S.News & WORLD REPORT RANKINGS



Marist has been included in The Princeton Review for 13 years in a row.

Kiplinger

For eight straight years, *Kiplinger's Personal Finance* has ranked Marist among "100 Best Buys in Private Colleges."



25 Best BACHELOR'S INFORMATION TECHNOLOGY PROGRAMS

NSF

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

The Princeton Review Forbes

25 Most Connected Campus

Marist Security Operations Center (SOC)

- Grand opening September 2018
  - 4 large screen (72”) computers and 32 desktops (both Windows and Mac hardware at each desktop)
  - Time delayed live data from Marist campus and CCAC security systems
  - Cloud Security and Graph Analytics
    https://www.youtube.com/watch?v=Hz_XyIipC2Y&feature=youtu.be
  - Cybersecurity education, Geolocation, and IBM Qradar
    https://www.youtube.com/watch?v=VZo9TWKIAbI&feature=youtu.be

Background

- The Internet of Things (IoT) has not been around for a long time, but it has evolved at an incredible pace.
- Steve Leibson stated that “The address space expansion means that we could assign an IPV6 address to every atom on the surface of the Earth and still have enough addresses left to do another 100+ Earths” [2].
- Cisco estimates that by 2020 there will be 50 billion devices in the IoT [3].
- The devices included in the IoT have become more prevalent in our everyday lives which brings up security and privacy concerns.
- Common security vulnerabilities include weak passwords, little or no data encryption, and insecure GUIs.
- Just these vulnerabilities alone can lead to major security breaches.
- Vulnerable IoT devices can be compromised by malware and be used as spam relays, cryptocurrency miners, and botnets, such as the Mirai botnet.
- One family’s Nest camera was recently hacked and used to belt out a fake emergency message about an impending missile strike from North Korea using the Nest Cam’s built-in speaker[5].

Disclaimer

- The security breach techniques demonstrated in this class should never be used on the Internet, or any public or private network. These examples are used for illustration purposes only. Your professor and the college do not assume any liability if you use these techniques outside of class, even if you claim to be “just practicing the course material”.

- In other words, ***don’t try this at home !!!***

Marist Internet of Things (IoT) Research Lab

Cybersecurity research including:

- Smart homes & speech recognition (Google Home, Amazon Alexa)
- Digital health care & remote patient monitoring (heart rate, blood pressure, blood oxygen, and more)
- Routers, Hubs, and Security Appliances
- Hardware & Software Design (Arduino, Raspberry Pi)
- Networked Devices (smart light bulbs, doorbells, thermostats, wall outlets, air quality monitors)
- Wireless penetration testing (AirPCap, Wifi Pineapple, RFID tags, botnets)

MARIST

INTERNET of THINGS

RESEARCH LAB

NSF

BlackRidge TECHNOLOGY

IBM

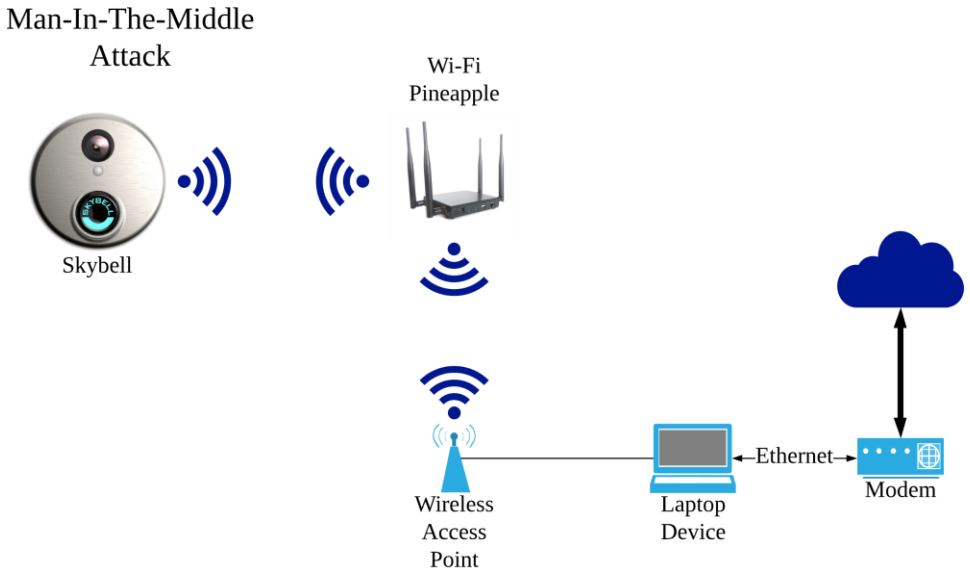
Experimental Setup

- The main technologies we are using for this project are the Ring Video Doorbell Ver. 2, Nest Doorbell, and Skybell
- The WiFi feature in these devices are attractive to consumers because its easy to install and connect to them. This ease of use is a problem because it does not allow for strong encryption and weak security [1].

Experimental Setup

- This project looks into the security vulnerabilities identified from testing three smart doorbells currently on the market (Skybell, Ring, and Nest).
- Experiments include reconnaissance using port scans and man-in-the-middle attacks using a rogue access point to intercept the packets being transmitted.
- We will use hacking technologies readily available on the market such as the WiFi Pineapple Tetra, WireShark, and Aircrack-ng to penetrate the doorbell systems.

Network Diagram



Network Diagram of the experimental setup for the Man-In-The-Middle attack on the Skybell device

Procedure

- We collected packets using the SiteSurvey module from the WiFi Pineapple Tetra and analyzed them with WireShark.
- Through the use of the WiFi Pineapple Site Survey module we were first able to find out information about the network(IOTLAB) all the devices are connected to.
  - Encryption: WPA2, Cipher: CCMP, Auth: PSK, Channel: 5, Frequency: 2.432
- Within this module we are able to deauthorize the devices on the network. The deauthorization attack disconnects the smart doorbells on the IOTLAB network and allows the WiFi Pineapple to capture the files being exchanged between the access point and the devices.
- Before deauthorizing the packets we collected multiple capture files to see what the devices were on the network.
- The capture files we collected were analyzed using Wireshark.

WireShark Scan

SamsungE_35:f2:29	Skybell_08:1b:a2	EAPOL	133	Key (Message 1 of 4)
Skybell_08:1b:a2	SamsungE_35:f2:29	EAPOL	155	Key (Message 2 of 4)
SamsungE_35:f2:29	Skybell_08:1b:a2	EAPOL	189	Key (Message 3 of 4)
Skybell_08:1b:a2	SamsungE_35:f2:29	EAPOL	133	Key (Message 4 of 4)

206	-0.000016		Skybell_08:1b:a2 (d0:c1:93:08:1b…	802.11	10	Clear-to-send, Flags=........
207	-0.000001	SamsungE_35:f2:29 (2c:ba:ba:35:f2:29)…	Skybell_08:1b:a2 (d0:c1:93:08:1b…	802.11	28	802.11 Block Ack, Flags=........
208	0.003601	Skybell_08:1b:a2 (d0:c1:93:08:1b:a2) …	SamsungE_35:f2:29 (2c:ba:ba:35:f…	802.11	28	802.11 Block Ack, Flags=........
209	0.001024	Skybell_08:1b:a2 (d0:c1:93:08:1b:a2) …	SamsungE_35:f2:29 (2c:ba:ba:35:f…	802.11	16	Request-to-send, Flags=........
210	0.012784		Skybell_08:1b:a2 (d0:c1:93:08:1b…	802.11	10	Clear-to-send, Flags=........
211	0.000000	SamsungE_35:f2:29 (2c:ba:ba:35:f2:29)…	Skybell_08:1b:a2 (d0:c1:93:08:1b…	802.11	28	802.11 Block Ack, Flags=........
212	0.793131		1c:f2:9a:c3:ee:f1 (1c:f2:9a:c3:e…	802.11	10	Acknowledgement, Flags=........
213	0.002050		1c:f2:9a:c3:ee:f1 (1c:f2:9a:c3:e…	802.11	10	Acknowledgement, Flags=........

- After we ran deauthorization to ensure that all the doorbell devices where disassociated from the network.
- We collected the files after we turned deauthorization on and off.
- By using this method we were able to collect the WPA keys for the Skybell and Ring as well as for a device using LGInnotek and Duratech.
- After finding the WPA key nonce for the Ring doorbell I was able to decrypt the keys using wireshark. By doing this I was able to find an IP address for the Ring doorbell and run an nmap scan.

- Search Wireshark using filter eth.dst == F0:C7:7F:C4:21:A4
- Notice Session Initialization Protocol (SIP) is initiated at frame 1516.
- SIP is a communications protocol for signaling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls, in private IP telephone systems, as well as in instant messaging over Internet Protocol (IP) networks.

RingVideoDoorBell.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.dst == F0:C7:7F:C4:21:A4

No.	Time	Source	Destination	Protocol	Length	Info
1177	11.830353	192.168.1.51	192.168.1.77	UDP	50	56934 → 838 Len=8
1178	11.833794	192.168.1.51	192.168.1.77	UDP	50	56935 → 902 Len=8
1187	12.028513	192.168.1.51	192.168.1.77	UDP	50	56936 → 903 Len=8
1188	12.132512	192.168.1.51	192.168.1.77	UDP	43	56893 → 764 Len=1
1243	12.439604	192.168.1.51	192.168.1.77	UDP	92	65063 → 989 Len=50
1335	12.686565	192.168.1.51	192.168.1.77	UDP	43	56894 → 767 Len=1
1336	12.686637	192.168.1.51	192.168.1.77	UDP	43	56895 → 772 Len=1
1372	13.279568	192.168.1.51	192.168.1.77	UDP	90	56884 → 687 Len=48
1464	14.327650	192.168.1.51	192.168.1.77	UDP	90	56888 → 688 Len=48
1465	14.327728	192.168.1.51	192.168.1.77	UDP	90	56889 → 689 Len=48
1466	14.327759	192.168.1.51	192.168.1.77	UDP	43	56898 → 773 Len=1
1467	14.327787	192.168.1.51	192.168.1.77	UDP	43	56899 → 774 Len=1
1468	14.327816	192.168.1.51	192.168.1.77	UDP	43	56900 → 775 Len=1
1469	14.331530	192.168.1.51	192.168.1.77	UDP	50	56940 → 944 Len=8
1473	14.387627	192.168.1.51	192.168.1.77	SSL	109	Client Hello
1474	14.387696	192.168.1.51	192.168.1.77	SSL	109	Client Hello
1475	14.387734	192.168.1.51	192.168.1.77	UDP	106	56823 → 686 Len=64
1476	14.387763	192.168.1.51	192.168.1.77	UDP	50	56941 → 959 Len=8
1516	14.480634	192.168.1.51	192.168.1.77	SIP	271	Request: OPTIONS sip:nm |
1517	14.480696	192.168.1.51	192.168.1.77	SIP	271	Request: OPTIONS sip:nm |
1518	14.480726	192.168.1.51	192.168.1.77	SIP	271	Request: OPTIONS sip:nm |
1519	14.480752	192.168.1.51	192.168.1.77	UDP	50	56944 → 965 Len=8
1569	15.194635	192.168.1.51	192.168.1.77	UDP	50	56945 → 983 Len=8

```
Frame 1473: 109 bytes on wire (872 bits), 109 bytes captured (872 bits)
Ethernet II, Src: Dell_c7:d0:cd (00:1a:a0:c7:d0:cd), Dst: TexasIns_c4:21:a4 (f0:c7:7f:c4:21:a4)
Internet Protocol Version 4, Src: 192.168.1.51, Dst: 192.168.1.77
User Datagram Protocol, Src Port: 56812, Dst Port: 684
Datagram Transport Layer Security
```

Nmap Scan

We also found that the Ring is under the name as Texas Instrument by connecting the MAC address from the box the device comes in and from looking it up in Wireshark.

The Ring doorbell has an internal battery, which can be accessed from outside the housing by removing one screw. This makes it more susceptible to physical attack than the other doorbells.

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-03
19:03 Eastern Daylight Time
Nmap scan report for Ring.lan (              )
Host is up (0.010s latency).
All 1000 scanned ports on Ring.lan (              ) are
closed
MAC Address:                    (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 9.83
seconds
```

Ring Doorbell

- Ring uses the following ports:
- TCP 80 TCP 443 TCP & UDP 15063 UDP range between 16500-32768 UDP 51504/51506
- Ports can be “opened” or “closed” on your router’s firewall. Open ports allow devices to send information through them, while closed ports block all traffic. Ring products only function properly if the required ports are open outbound from your router. The process to open ports can be different, depending on your type of router. Consult your router’s user manual for instructions on how to open ports.
- Ring Chime also requires certain ports. If your Chime is not ringing, ensure that the following ports are open outbound as well:
- TCP 80 TCP 443 TCP 9998 TCP 9999
- The client applications also use the following inbound ports:
- TCP 7078 TCP 9078

Securing IoT Devices

- We have experimented with secure authentication to IoT devices and other equipment using a combination of First Packet Authentication and Transport Access Control techniques.

Identity-Based Network Security for the Cloud: First Packet Authentication & Transport Access Control

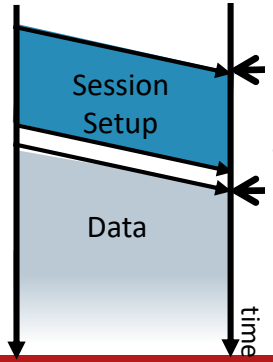
- Networks do not allow for user or device identity to be determined before establishing network connections
- BlackRidge Transport Access Control (TAC) authenticates identity and enforces security policy on the first packet, **before a network session is established, by inserting a time-limited, 64 bit ID token into the packet header.**

Caller-ID for the Internet

Before caller-ID, you needed to answer to determine identity.

After caller-ID, you only answer authenticated and authorized callers.

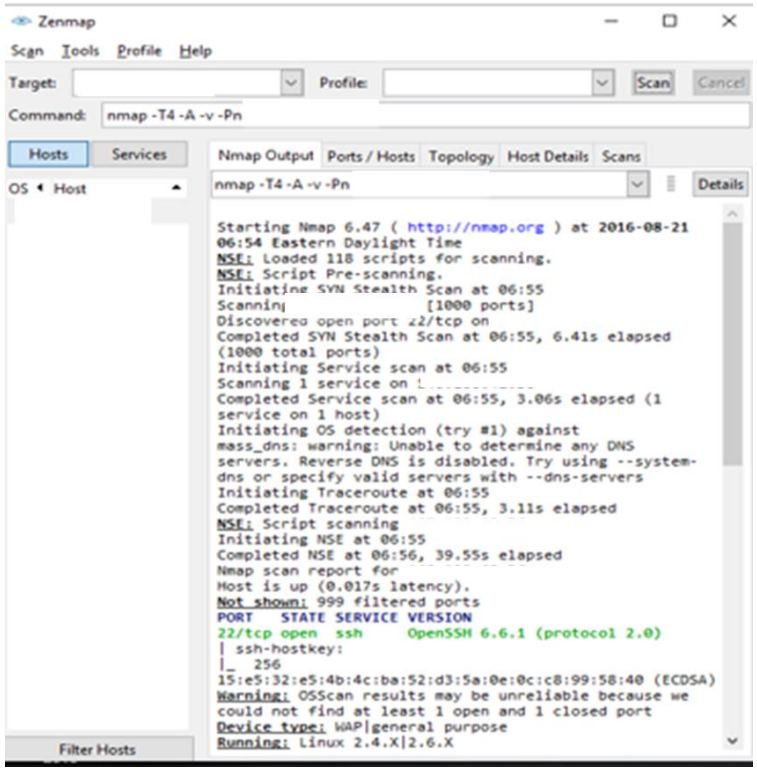
First Packet Authentication

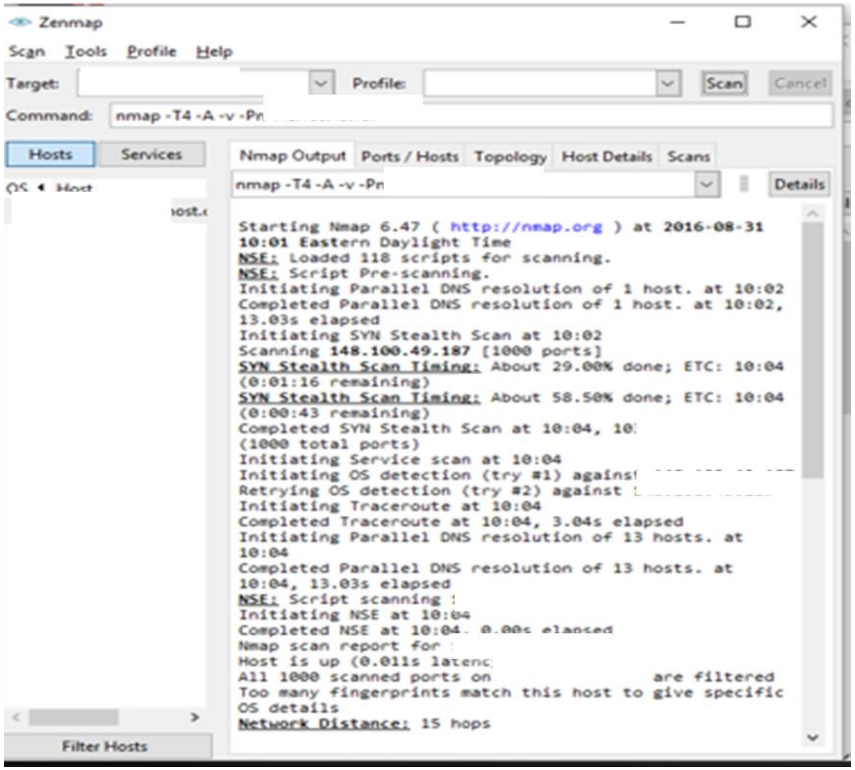


First Packet Authentication stops unauthorized access at the earliest possible time.

Current security products start after network sessions are established.

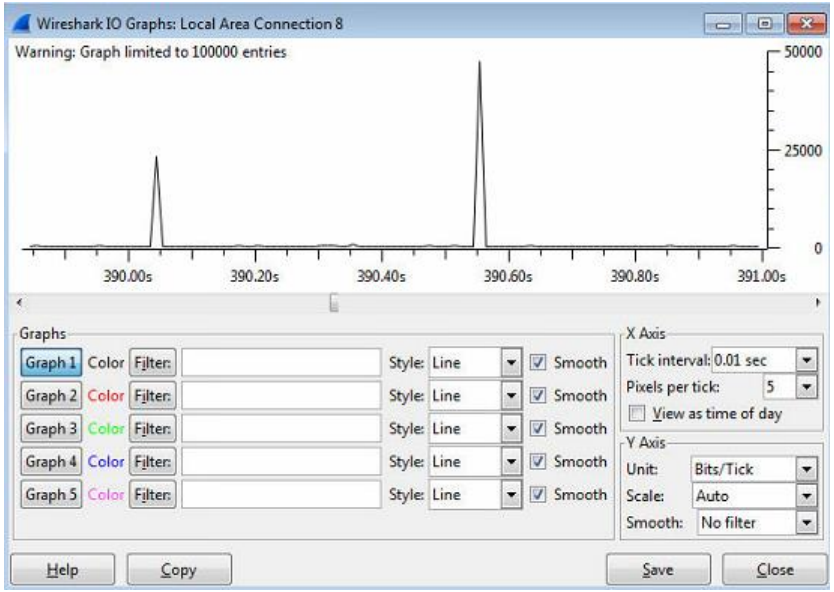
Network scan before & after implementing TAC

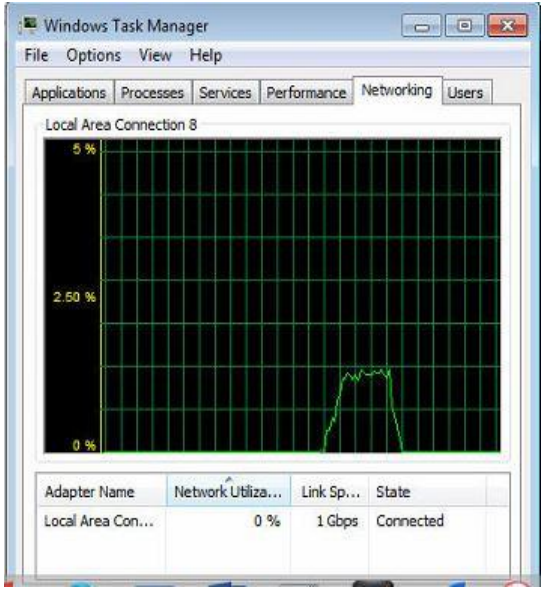




Marist BlackRidge Syslog Rate testing

10 messages 5 sec rate limit 5 Mbps ***no rate limit up to 14 Mbps***





50,000 bits in 0.01 sec, 100 x 50,000=5,000,000 bps = 5 megabits / sec
1.4% of 1gig = 14 megabits / sec

Marist BlackRidge Protect Against IoT Threats

Trustedad
Group trustedad

A BlackRidge Trusted user with identity attempts to access a server it is not authorized for

After 3 unauthorized attempts, Trusted traffic is discarded

Protected29
Group trustedad

Gateway4
Port 1 Port 2

Management
Port 4

Marist Network

Gateway5
Port 1 Port 2

Management
Port 4

Level	Policy
5	Forward
4	Restricted Applications
3	Redirect
2	Drop

Orchestrator calls Gateway REST API to lower trust level by 1

BlackRidge Gateway sends Unauthorized Syslog entry to Graylog

Resource not authorized for user Trustedad

Orchestrator

Graylog HTTP POST alert message to Orchestrator

graylog

Research SOC

BlackRidge TECHNOLOGY

Conclusions

- We have experimentally evaluated three popular smart doorbell brands
- It was possible to observe device handshakes with a local wi-fi router and run MITM attacks using deauthentication
- It should be possible to record and replay short video clips to make it seem as if nobody is present
- Further IoT research is ongoing

Thank You

Follow @Dr_Casimer or http://www.ofcconference.org/en-us/home/about/ofc-blog/
or visit the Marist Innovation Lab on GitHub: https://github.com/Marist-Innovation-Lab

References

- [1] Lewis, James A. Managing risk for the Internet of Things. Washington: Center for Strategies & International Studies, 2016.
- [2] Foote, Keith. "A Brief history of the Internet of Things." Dataversity, https://www.dataversity.net/brief-history-internet-things/
- [3] Evans, Dave. The Internet of Things: How the Next Evolution of the Internet is Changing Everything. San Jose: Cisco Internet Business Solutions Group (IBSG), 2011
- [4] Chang, Lulu. "A Ring doorbell vulnerability lets people snoop even after a password change." Digital Trends, https://www.digitaltrends.com/home/ring-video-doorbell-security-exploit/
- [5] Gafni, Matthias. ""5 minutes of sheer terror": Hackers infiltrate East Bay family's Nest surveillance camera, send warning of incoming North Korea missile attack." The Mercury News. https://www.mercurynews.com/2019/01/21/it-was-five-minutes-of-sheer-terror-hackers-infiltrate-east-bay-familys-nest-surveillance-camera-send-warning-of-incoming-north-korea-missile-attack/

Conference Presentations

- M. Molenaer, M. Barbieri, V. Joseph, M. Crawley, and P. Liengtiraphan, “Zero Trust Networks using Transport Access Control Techniques” Proc. IBM TechConnect (Best of Solutions Award, Early Tenure Category), IBM Poughkeepsie/Yorktown Heights, NY (September 22, 2016)
- P. Liengtiraphan and C. DeCusatis, “Zero Trust Networks using Transport Access Control and First Packet Authentication”, Proc. NYIT 6th Annual Cybersecurity Conference, New York, NY, student poster session (Sept. 22, 2016) http://www.nyit.edu/events/annual_cybersecurity_conference
- C. DeCusatis, “Cloudy with a chance of SDN Part II”, BRKCRT-2603, Cisco Live, Las Vegas, NV (July 10-15, 2016)
- C. DeCusatis, “The NSF SecureCloud project: cybersecurity for enterprise class data centers”, Proc. NSF Enterprise Computing Conference (ECC), Marist College, Poughkeepsie, NY, June 12-14, 2016
- C. DeCusatis, “Zero trust cybersecurity architectures for software defined data centers”, Proc. NYSERNET (Internet 2) Tech Summit, Vassar College, Poughkeepsie, NY June 16-17, 2016
- R. Cannistra, P. Liengtiraphan, and V. Joseph, "Securing SDN and NFV Enabled Campus Environments through Orchestration and Automation", Proc. Internet 2 Technology Exchange, Miami, FL (September 2016)
- P. Liengtiraphan and V. Joseph, “How to make a honeypot”, lightning talk presented at Internet 2 Technology Exchange, Miami, FL (September 2016)

Conference Presentations

- C. DeCusatis, D. Eidle, S. Ni, B. Ross, M. Miller, and B. Traditi, “Autonomic security: real time response to cybersecurity threats”, Proc. NYIT 7th Annual Cybersecurity Conference, New York, NY (Sept. 23, 2017) http://www.nyit.edu/events/annual_cybersecurity_conference (last accessed September 2017)
- C. DeCusatis, A. Labouseur, T. Famularo, J. Heiden, G. Leaden, T. Magnusson, and M. Zimmermann, “An API Honeypot for DDoS and XSS Analysis”, Proc. NYIT 7th Annual Cybersecurity Conference, New York, NY; Best Undergraduate Research Paper Award (Sept. 23, 2017) http://www.nyit.edu/events/annual_cybersecurity_conference (last accessed September 2017)
- D. Eidle, S. Ni, C. DeCusatis, and A. Sager, “Autonomic security for zero trust networks”, Proc. IEEE 8th annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), Columbia University, New York, NY (Oct. 19-21, 2017)
- G. Leaden, M. Zimmermann, C. DeCusatis, and A. Labouseur, “An API Honeypot for DDoS and XSS Analysis”, Proc. IEEE/MIT Undergraduate Research Technology Conference, Cambridge, MA (Nov. 3-5 2017)
- C. DeCusatis, M. Zimmerman, and A. Sager, “Identity based network security for commercial Blockchain services“, Proc. 8th annual IEEE Computing and Communications Workshop and Conference, Las Vegas, NV (January 8-10, 2018)

Research Papers

- S. Nanda, F. Zafari, C. DeCusatis, E. Wedaa and B. Yang, “Predicting Network Attack Patterns in SDN using Machine Learning Approach”, Proc. IEEE 2016 Conference on Network Function Virtualization and Software Defined Networks (SDN/NFV 2016), Palo Alto, CA (Nov. 7-9, 2016) http://nfvsdn2016.ieee-nfvsdn.org/
- C. DeCusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, “Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication”, Proc. IEEE International Conference on Smart Cloud (SmartCloud 2016), New York, NY (Nov. 18-20, 2016) http://csis.pace.edu/CSCloud/sc2016/
- C. DeCusatis, A. Carranza, “Modeling software defined networks using Mininet”, Proc. 2nd International Conference on Computer and Information Science and Technology (CIST), Montreal, Canada (May 20-21, 2016) (Best Paper Award)
- C. DeCusatis, K. Lotay, “Secure, decentralized energy resource management using the Ethereum blockchain”, Proc. IEEE Trustcon 2018, International Workshop on Cyber-Physical Systems, pp. 1-7, New York, NY (August 2-5, 2018)
- C. DeCusatis, “The NSF SecureCloud project: cybersecurity for autonomic, zero trust networks”, Proc. NSF Internet 2 Cybersecurity Transaction to Practice Workshop, City University of New York, NY (April 17, 2018)