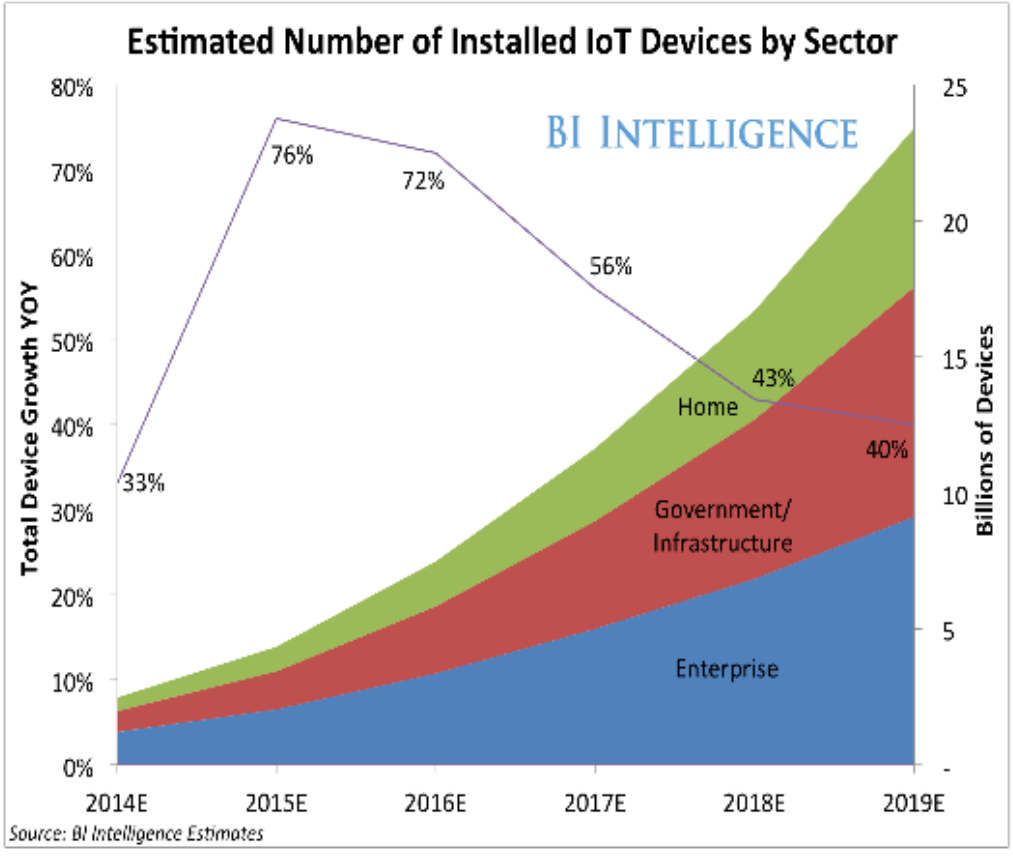
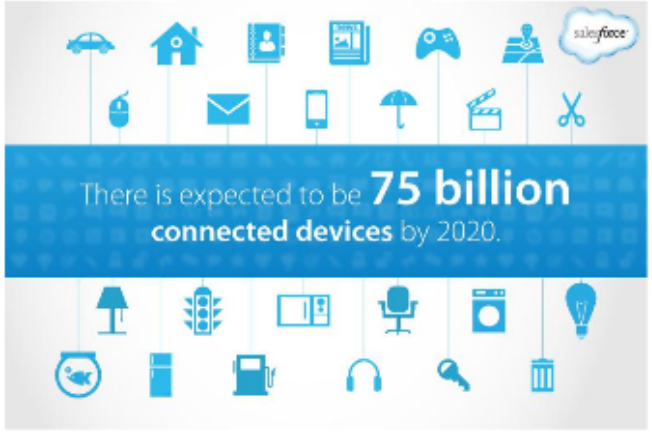
Is Anybody Home? Inferring Activity from Smart Home Network Traffic

Bogdan Copos Matt Bishop Karl Levitt Jeff Rowe

University of California, Davis

UCDAVIS


Estimated Number of Installed IoT Devices by Sector
BI INTELLIGENCE
Total Device Growth YOY
Billions of Devices
80%
70%
60%
50%
40%
30%
20%
10%
0%
25
20
15
10
5
-
76%
72%
56%
43%
40%
33%
Home
Government/
Infrastructure
Enterprise
2014E
2015E
2016E
2017E
2018E
2019E
Source: BI Intelligence Estimates


There is expected to be 75 billion
connected devices by 2020.


U.S. Unit Sales of
Smart Home Devices*
MILLIONS OF UNITS
40
20
0
2014
2015
2016
2017
* Smart thermostats, networked cameras, smart door locks, smart water leak detectors, smart smoke detectors, smart carbon monoxide detectors, and smart light bulbs, smart light switches, smart plugs and outlets, and smart power strips
© Parks Associates

UCDAVIS

UCDAVIS

Samsung Smart Home flaws let hackers make keys to front door

Don't rely on SmartThings for anything security related, researchers warn.

by **Dan Goodin** - May 2, 2016 11:31am PDT

Samsung Smart Home flaws let hackers make keys to front door

Don't rely on Sma

by **Dan Goodin** - May 2,

KIM ZETTER SECURITY 01.05.16 7:00 AM

XFINITY'S SECURITY SYSTEM FLAWS OPEN HOMES TO THIEVES

eet Email 61

Samsung Smart Home flaws let hackers make keys to front door

Don't rely on Sma

by **Dan Goodin** - May 2,

KIM ZETTER SECURITY 01.05.16 7:00 AM

XFINITY'S SECURITY SYSTEM FLAWS OPEN HOMES TO

eet Email 61

For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

Julie Bort

Jan. 16, 2014, 1:36 PM 197,861 39

Samsung Smart Home flaws let hackers make keys to front door

Don't rely on Sma

by **Dan Goodin** - May 2,

KIM ZETTER SECURITY 01.05.16 7:00 AM

XFINITY'S SECURITY SYSTEM FLAWS OPEN HOMES TO

eet Email 61

For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

Hello, Dave. I control your thermostat. Google's Nest gets hacked

DEAN TAKAHASHI AUGUST 10, 2014 8:00 AM


Samsung Smart Home flaws let hackers make keys to front door
Don't rely on Sma
by Dan Goodin - May 2,
KIM ZETTER SECURITY 01.05.16 7:00 AM
XFINITY'S SECURITY SYSTEM
FLAWS OPEN HOMES TO
eet
Email
61
For The First Time, Hackers Have Used A Refrigerator To Attack Businesses
Hello, Dave. I control your thermostat. Google's Nest gets hacked
ANDY GREENBERG SECURITY 07.21.15 6:00 AM
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Samsung Smart Home flaws let hackers make keys to front door

Don't rely on Sma

by Dan Goodin - May 2,

KIM ZETTER SECURITY 01.05.16 7:00 AM

XFINITY'S SECURITY SYSTEM FLAWS OPEN HOMES TO

eet Email 61

For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

Hello, Dave. I control your thermostat. Google's Nest gets hacked

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

CNET › Security › Hello Barbie: She's just insecure

Hello Barbie: She's just insecure

Researchers revealed new flaws in the doll Friday, adding to problems publicized last week. Hello Barbie's software maker is racing to patch security bugs during the holiday shopping season.

Samsung Smart Home flaws let hackers make keys to front door

Don't rely on Sma

by Dan Goodin - May 2,

KIM ZETTER SECURITY 01.05.16 7:00 AM

XFINITY'S SECURITY SYSTEM FLAWS OPEN HOMES TO

eet Email 61

For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

Hello, Dave. I control your thermostat. Google's Nest gets hacked

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

CNET › Security › Hello Barbie: She's just insecure

Hello Barbie: She's just insecure

Researchers revealed new flaws in the doll Friday, adding to problems publicized last week. Hello Barbie's software maker is racing to patch security bugs during the holiday shopping season.

Report: Thieves Can Hack and Disable Your Home Alarm System | WIRED

POSTED BY: PAUL JULY 23, 2014 10:16 COMMENTS OFF ON REPORT: THIEVES CAN HACK AND DISABLE YOUR HOME ALARM SYSTEM | WIRED

UCDAVIS

Security

Many things can go wrong...

- malicious firmware

  e.g. Nest hack presented at BlackHat '14

- poor authentication

  e.g. Rapid7 report on baby monitors hacks

- communication hack

  e.g. Xfinity Home Security System jamming hack

- compromised cloud

  nothing yet?

- **data inference**

UCDAVIS

Traffic Analysis

The process of analyzing network traffic for inferring information about the device and its state

- packet/connection size
- protocol
- source/destination address
- timing information
- burstiness

Background

Traffic Analysis:

- Web Browsing
- Marketing
- Reconfiguring Networks
- Monitoring

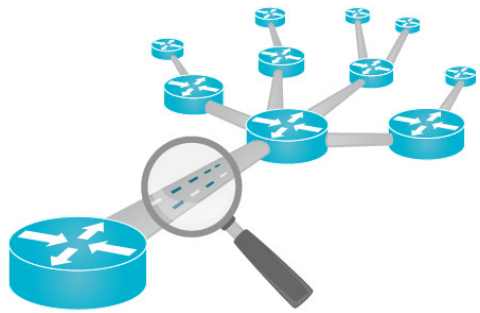
IoT/Smart Home Devices:

- "**Extrapolation and prediction of user behaviour from wireless home automation communication**"

  F. Mollers et al (WiSec '14)
- "**Smart Nest Thermostat: A Smart Spy in Your Home**"

  G. Hernandez (BlackHat '14)
- "**Security Analysis of Emerging Smart Home Applications**"

  E. Fernandes et. al. (S&P '16)



UCDAVIS

Devices

- Nest Thermostat 2nd Generation
  - remotely control temperature
  - motion detector
  - self-learning schedule
  - interface for settings and usage logs
  - 802.15.4 radio
- Nest Protect 2nd Generation
  - motion detector
  - Pathlight
  - Nest Interconnect
  - 802.15.4 radios

UCDAVIS

Problem Statement

What does network traffic tell us about the devices (and their state)?

Problem Statement

What does network traffic tell us about the devices (and their state)?

Can network traffic be used to infer state of building?

UCDAVIS

Events of Interest

1. Nest Thermostat mode
   - Home
   - Auto-Away

Events of Interest

1. Nest Thermostat mode
   - Home
   - Auto-Away

2. Nest Protect Pathlight Activation

Events of Interest

1. Nest Thermostat mode
   - Home
   - Auto-Away
2. Nest Protect Pathlight Activation
3. Nest Protect Smoke Alarm

Setup

HP netbook

Network interface in monitor mode

dumpcap with MAC address based filter

Approximately 1 month of pcaps

Convert pcaps to connection logs using *Bro*

User Activity

User activity during time of packet captures varies:

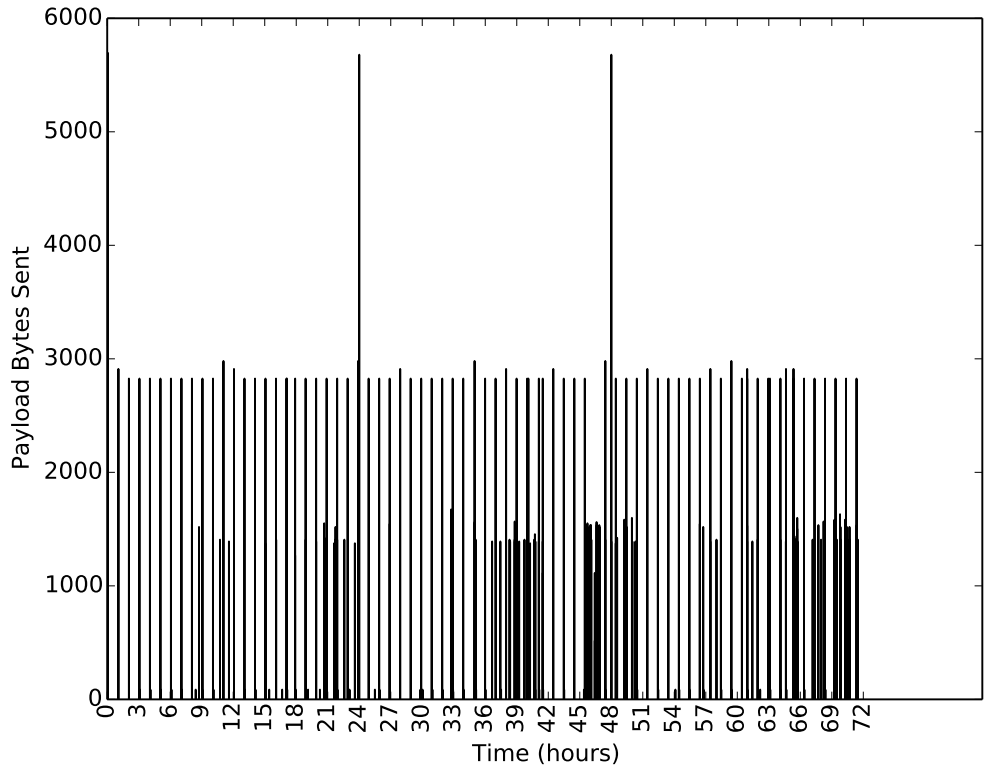
- time of arrival
- time of departure
- number of arrivals & departures

Traffic Overview

Nest Thermostat

- 14 hosts
- HTTP, **NTP**, DNS, SSL/TLS

HTTP used to obtain weather data



Correlation Analysis

Supervised correlation analysis to identify connections (up to set of three connections) which occur only during the time of an event.

1. Extract time of events (i.e. *ground-truth*)

Correlation Analysis

Supervised correlation analysis to identify connections (up to set of three connections) which occur only during the time of an event.

1. Extract time of events (i.e. *ground-truth*)

2. Parse *connection logs* and extract connections

Correlation Analysis

Supervised correlation analysis to identify connections (up to set of three connections) which occur only during the time of an event.

1. Extract time of events (i.e. *ground-truth*)

2. Parse *connection logs* and extract connections

3. For each type of event, generate frequency count per connection

Correlation Analysis

Supervised correlation analysis to identify connections (up to set of three connections) which occur only during the time of an event.

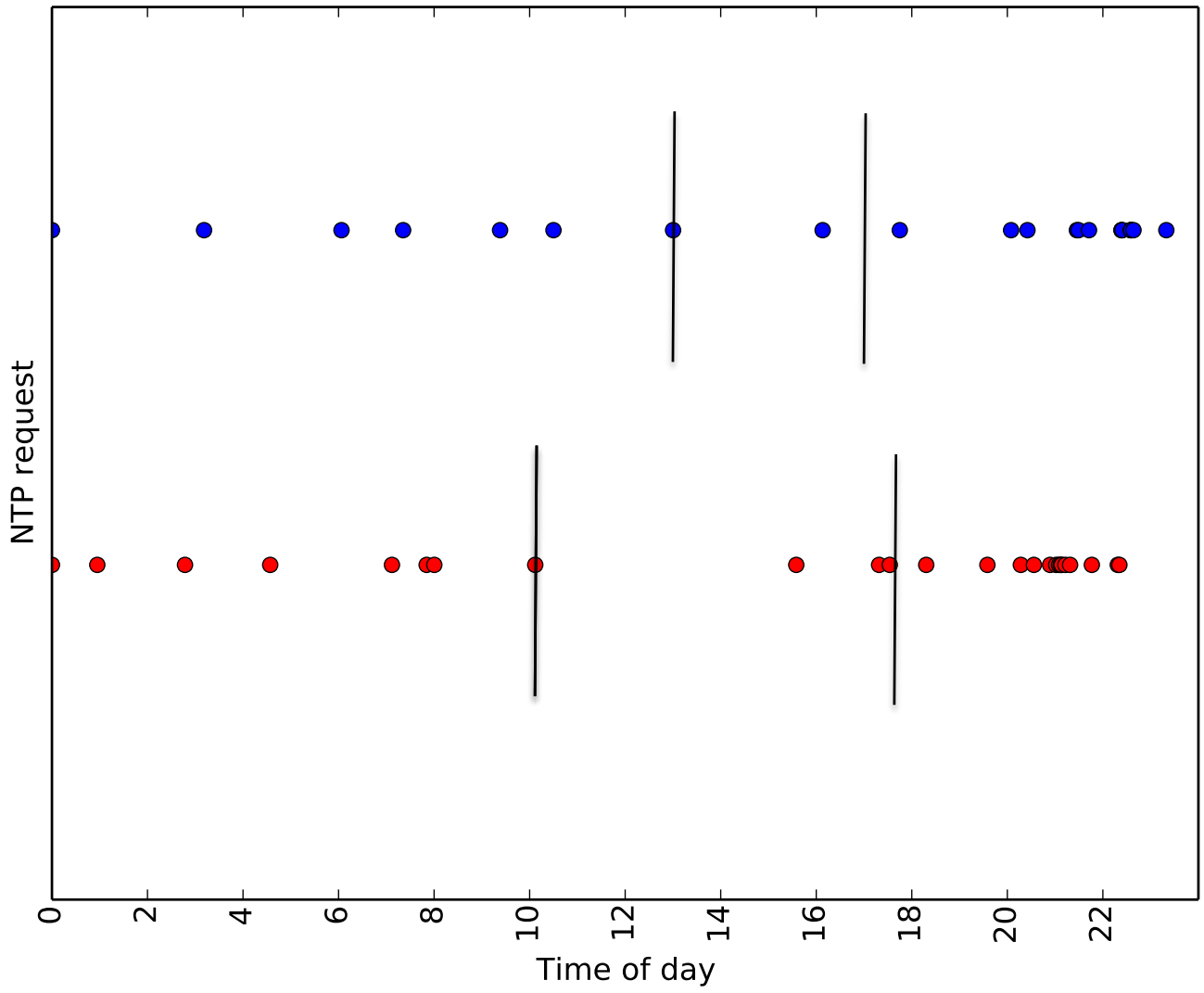
1. Extract time of events (i.e. *ground-truth*)
2. Parse *connection logs* and extract connections
3. For each type of event, generate frequency count per connection
4. Identify connections with high correlations

UCDAVIS

Findings

- Mode Transition
  - *Home* $->$ *Auto-Away*: set of 3 connections
  - *Auto-Away* $->$ *Home*: single connection
  - NTP requests
- Pathlight Activation
- Smoke Alarm
  - set of 2 connections

NTP Traffic



UCDAVIS

Evaluation

- **Mode Transition**
  Home $->$ *Auto-Away*: 67% accuracy, 0 False Positives
  Auto-Away $->$ *Home*: 88% accuracy, 0 False Positives
- **NTP Requests**
  simple SVM approach (features = number of NTP requests per hour period)
  81% accuracy
- **Pathlight Activation**
  50% accuracy (100% sensitivity), 0 False Negative
  FP due to repeated connections after 30 minutes
- **Smoke Alarm**
  100% accuracy

UCDAVIS

Limitations

- lack of flexibility for connection sizes

Limitations

- lack of flexibility for connection sizes
- time dependency

Limitations

- lack of flexibility for connection sizes
- time dependency
- no WPA/WEP encryption

Limitations

- lack of flexibility for connection sizes
- time dependency
- no WPA/WEP encryption
- source of False Positives and False Negatives

UCDAVIS

What can be done?

Previously proposed countermeasures include:

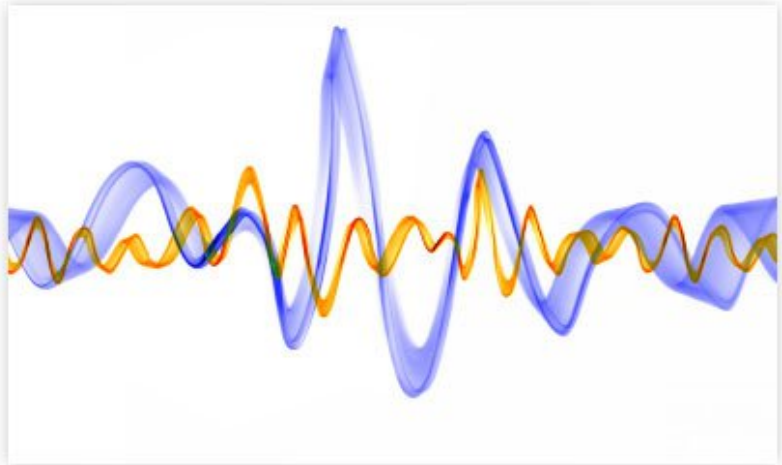
- Morphing
- Injecting Bogus Traffic
- Padding

BUT... **must** consider that IoT devices have limited resources

UCDAVIS

Future Work

- Apply signal processing techniques to model state of devices
- Study defense mechanisms



UCDAVIS

Thank you!

bcopos@ucdavis.edu

This work was made possible by the **RISE** project and **NSF SaTC**.

UCDAVIS