Let's Get Physical

Breaking Home Security Systems and Bypassing Buildings Controls

31 July 2013 – Black Hat USA 2013 – Las Vegas, NV

Presented by:
Drew Porter &
Stephen Smith
Bishop Fox
www.bishopfox.com

BISHOP FOX

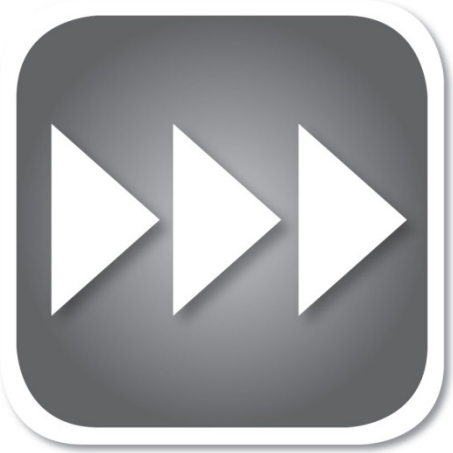
Agenda

OVERVIEW

- Demo
- Quick Overview
- Sensors
  - Door and window
  - Motion
- Keypads
  - Land line
  - Cellular
- Fixes
- Summary

Demo Time

LESS TALKING MORE DOING



Quick Overview

BACKGROUND

What We Really Focus on

PARTS TO TARGET

- Door and window sensors
- Motion detectors
- Keypads

BISHOP FOX

Security Systems

THE BASICS

- 2 functions
  - Deter intruders
  - Alert
- 3 parts
  - Door and window sensors
  - Motion Detector
  - Keypad

BISHOP FOX

Quick Facts

PHYSICAL SECURITY

- 5 – 20 year lifecycle

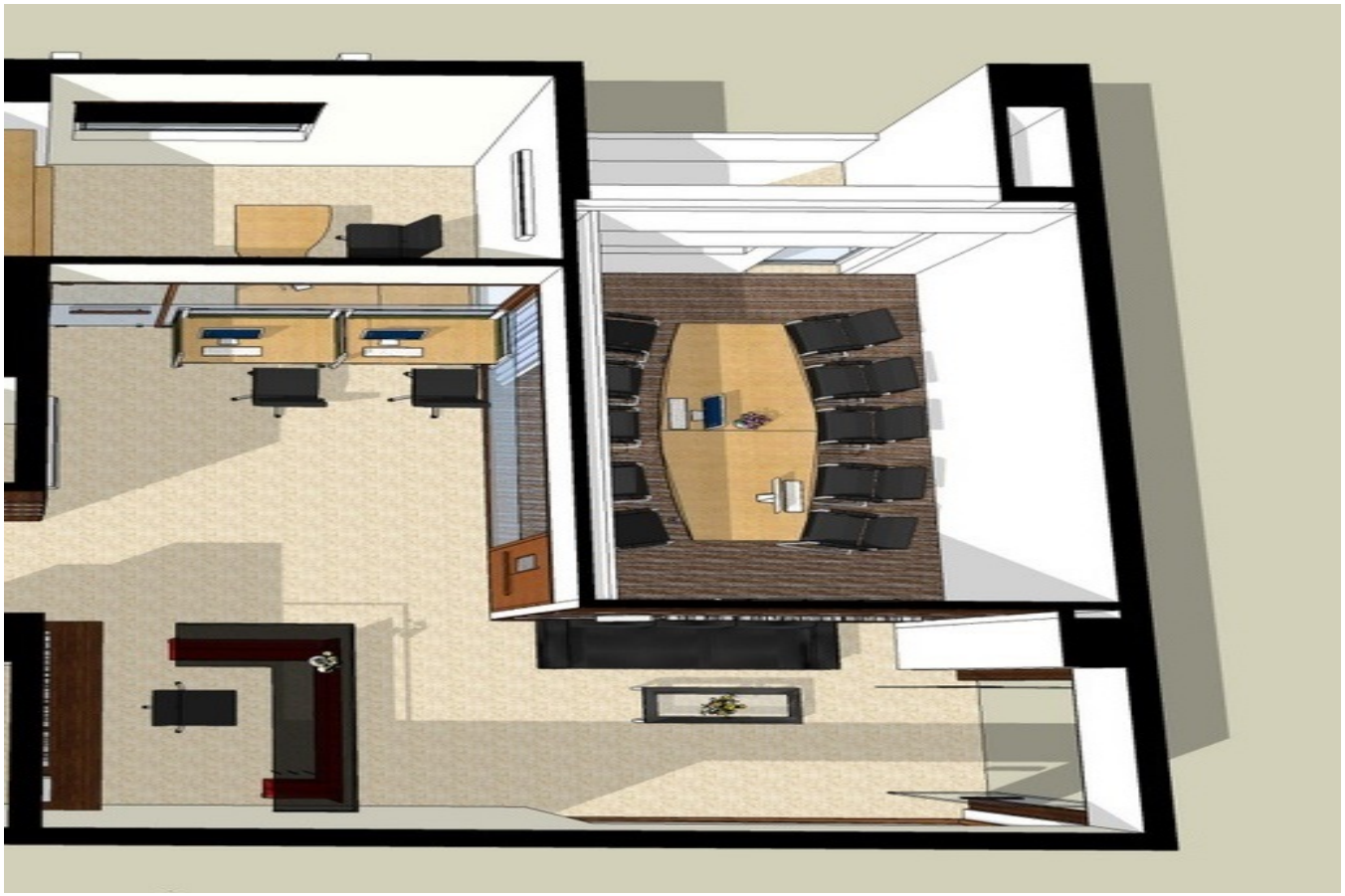
- Security items are broken
  - No one wants to hear about it

- Systems built to be cheap
  - Leads to higher tolerance devices
    - Easier to bypass

- Physical assessments are more common
  - Not just getting past locks anymore

Basic Office Setup

LAY OF THE LAND



BISHOP FOX

Sensors

HOW THEY WORK

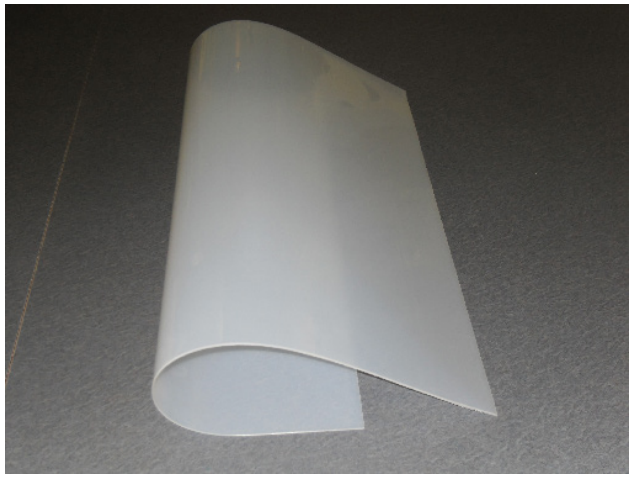
Door & Window

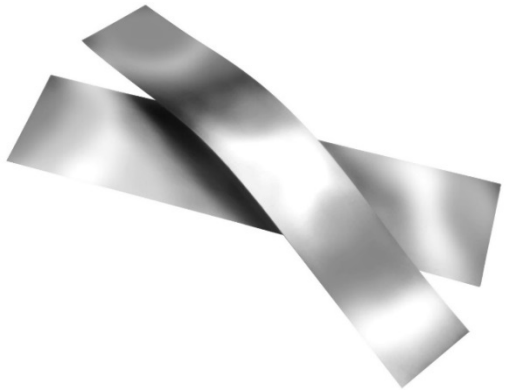
THE FACTS

- Most Basic Sensor
- Few Types
  - Wire or wireless
    - Magnetic and ball
- Same Basic Principle
  - Break the circuit = trip the alarm

Door & Window

DEFEATING THE SENSORS

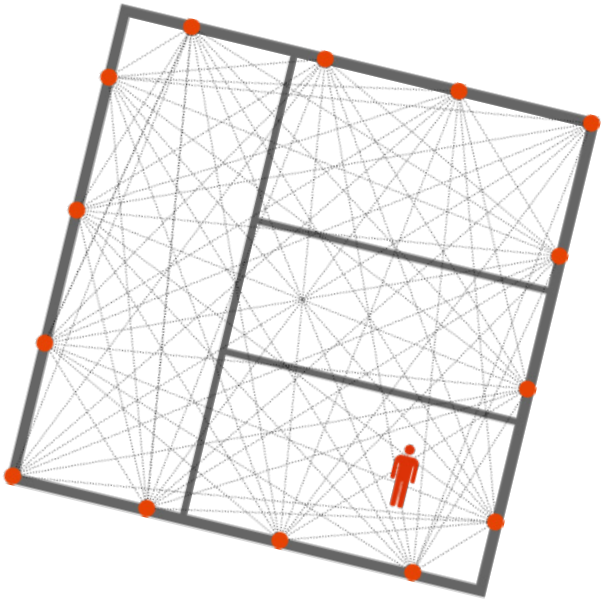




Motion

THE FACTS

- Ultrasonic
- Microwave
- Tomographic
- Passive infrared
  - Most common



Motion Continued

THE FACTS

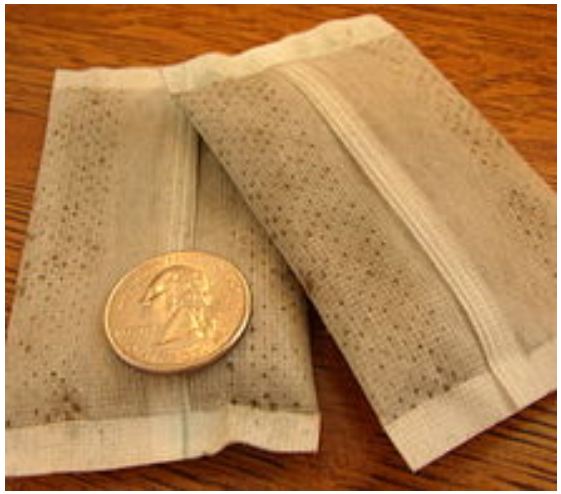
Dual tech

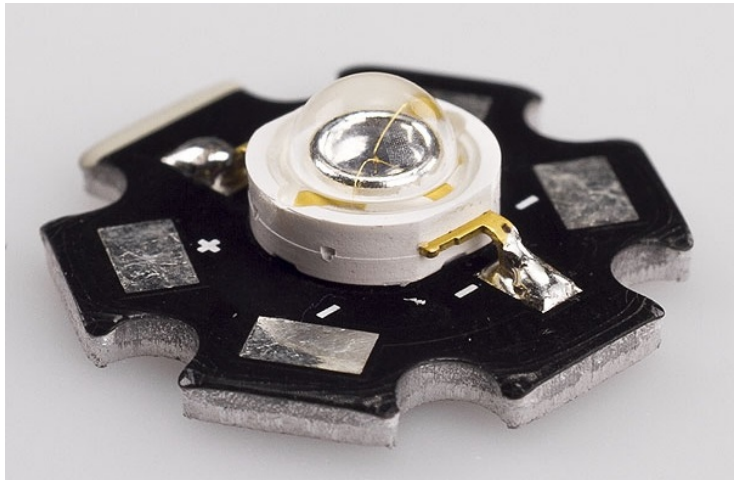
- Microwave + passive infrared
  - Most common
- Both tech have to trip to open the circuit
- Mostly in office buildings
  - Can be used to get past another physical control mechanism (i.e.: RFID)

BISHOP FOX

Motion

DEFEATING THE SENSORS





Keypads

HOW THEY WORK

Keypads

THE FACTS

- The "brains" of the alarm system
- Reports to you or monitoring center
- Many different data connections
  - Landline
  - Broadband
  - Cellular
- Holy grail to pwn

Defeating Keypads

LANDLINES AND CELLULAR

Now What?

SOME SUGGESTIONS

A Few Fixes

CAN'T SOLVE EVERYTHING

Door and Window

- Sadly, kind of screwed on this one

Motion

- Location, location, location!
- Better sensors

Keypad

- Use dual tech for reporting
- Reporter service using secure protocols
- Verify all security features

Backup Plan

...JUST IN CASE

Key Highlights

IF YOU ONLY REMEMBER TWO THINGS

1. Many systems are vulnerable and easy to break
2. More awareness is needed

Thank You

Bishop Fox – see for more info:
http://www.bishopfox.com/resources/tools/