



# Default Password Conundrum

**Walter P. Opaska**  
**CISSP, CISA, CPA**



# Biography

- Over 35 years in IT security and audit
- A CISSP, CISA, and CPA
- Managed IT security projects and audits as a Federal government employee and contract
- Treasurer of the ISC2, Quantico, VA chapter



# Conundrum?

- Is the default password problem a conundrum?
- Definition
  - An insoluble, or difficult problem
  - Does the definition fit?
- Some security professionals disagree



# Conundrum?

- This presentation will try to answer the conundrum question by:
  - Outlining the default password problem
  - Explaining why the conundrum definition applies
  - Discussing contemporary issues.



# The Default Password Problem



# What are Default Passwords

- Built in logonid/password pairs
- Built into operating system, firmware, database or software
- Some “benign”
- Others very powerful
- On all platforms



# Uses

- Initial installations or upgrades.
- Support
  - Vendor
  - Helpdesk
- Sales demonstration
- Internet communications
  - The ANONYMOUS account
- Simplify programming by “hardcoding”



# Nature of Threat

- Can Cause Major Damage
  - Privileged Accounts
  - Magnified by the Internet
- Long Term Problem
- Exists in Many Environments
- Ubiquitous





# Where Found

- On all platforms
- Operating Systems -Unix/Linux root
- Routers, access points, switches, firewalls, and other network equipment
- Databases
- Web applications
- Industrial Control Systems (ICS) systems
- Other embedded systems and devices
- Remote terminal interfaces like Telnet and SSH
- Administrative web interfaces
- Cloud services – IBM Cloudmaster
- Home Appliances/Devices
- Internet of Things (IOT)



# Why Used

- Installation
- Customer Support
- Vendor Troubleshooting
- Internet communications
- Database communications
- Simplify development by "hardcoding"
  
- If default user ids and passwords are so useful, why are they a security problem?



# Why “Conundrum” Applies



# Default Password Security Problems

- Passwords widely known
- Exist on many commercial systems
- May carry high level privileges
- Often tightly integrated into operations
- Present on mission critical systems
- Frequently left unsecured at installation
- Mask audit trail, obscuring monitoring
- Hardcoded “ defaults difficult to remove
- Can be easily exploited; even by a novice



# Most Critical Vulnerabilities

Information available to anyone

- Ease of exploitation



# Default Passwords Attack Types

- Brute Force
- Dictionary Use
- Automated Attacks
- Complex Internet Attacks



# Default Password Information Sources

- Numerous Sources

- Vendor Manuals and Data

- Internet

- Books

- Information Systems Training

- These sources cause the problem to fester



# Seriousness

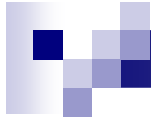
- SANS Institute
  - Recognized default passwords on its “Ten Most Critical Internet Security Threats
- OWASP
  - Part of OWASP Top 10 2013





# Authorities

- CERT Warning
  - Alert (TA13-175A)
  - Risks of Default Passwords on the Internet
- CAPEC
- NIST 800-53 IA-5
- OWASP Top 10 2013 – A5
- PCI DSS, Requirement 2
- DHS Alert (ICS-ALERT-13-164-01)



# Conundrum - Rationale

- Lasted for Decades
- From Mainframes to the Internet
- Numerous Platforms
- Morphed to Unexpected Areas



# Contemporary Default Password Issues



# A Contemporary Example

- Central Rappahannock Regional Library
- CRRL User Login Website
- Uses a Unique type of Default Password

# CRRL

Log In | Central Rappahannock Regional Library | BiblioCommons - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Log In | Central Rappahann... x +

https://librarypoint.bibliocommons.com/user/login

Most Visited FR SW Bookmarks Toolbar DR AA USSFCU

Help Log In / My CRRL

Central Rappahannock Regional Library  
INSPIRING LIFELONG LEARNING

Keyword

Advanced Search

Explore ▾ Collections ▾ Services ▾ Locations ▾ Events ▾ Research ▾ Kids ▾ Teens ▾

## Log In ?

**Username or Barcode:**

**PIN:**

Usually the last four digits of your phone number

[Forgot your PIN?](#)

Remember me on this device

Welcome to Your New Catalog!

Here's what's new...

- Find what you want with a better search.
- Track your borrowing.
- Rate and review titles you borrow, and share your opinions on them.
- Get personalized recommendations.

[Trouble logging in?](#)



# SCADA Systems

- Supervisory control and data acquisition
- Installed in utilities and manufacturing facilities to manage operations
- Major European SCADA manufacturer hardcoded known default passwords
- Targeted by malware
- Over 50 percent of SCADA suppliers hard-code passwords



# SCADA Systems (Continued)

- 10,500 small dish satellite systems vulnerable to cyber attacks
- very small aperture terminals, (VSATs)
  - Remote broadband Internet
  - Transmit PoS credit card transactions
- Many have default password settings



# Databases

- Databases have been plagued with default password security problems.
  - Oracle – dozens of default ids and passwords
- NoSQL databases have these problems
  - MongoDB had no passwords until 2015
  - After 2015 issue fixed
- MongoDB (older) databases subject to organized bitcoin ransom attempts



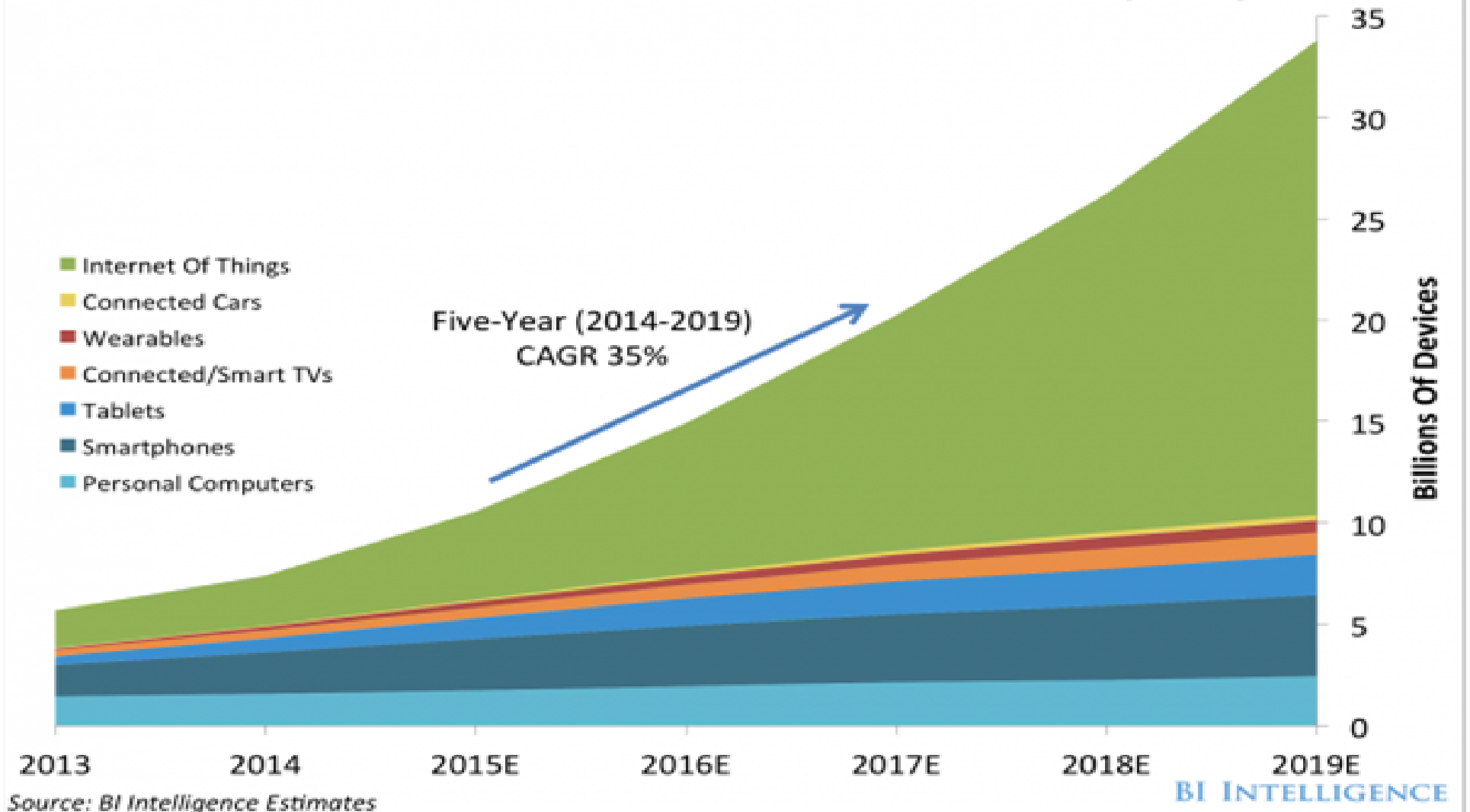


# Internet of Things (IoT)

- New dimension to default password
- Estimated 1.7 trillion industry by 2020
- Majority of IoT devices shipped to users
  - With default passwords
  - Already set by factory manufacturers
  - Source Mcafee.com

# 2017 - 20 Billion IoT Devices

## Number Of Devices In The Internet Of Everything





# IoT Devices with Default Passwords

- Cameras
- Printers
- DVR Recorders
- Cellular modems
- Solar panels
- Medical devices



# IoT DDoS and Defaults

- Two massive 2016 DDoS attacks enabled by IoT devices with default passwords
- Sept. 20 Akamai DDoS attack ,
  - Largest attack against company
- Oct. 20 attack Dyn US DNS Provider
  - Affected USA (East Coast)
  - Twitter, Amazon, Reddit, others affected
- Called the Mirai attacks



# Mirai Attack Characteristics

- DNS attacks using Mirai malware
- Originated from thousands of bots
  - Bots IoT cameras & DVRs
  - Used in homes & small office
  - Most from one Chinese manufacturer
- Devices use factory hardcoded default id/passwords
- Spread by scanning Internet for IoT devices with the default passwords.



# Attack Fixes

- Malware eliminated by power off
- Re-infection can easily reoccur
- Manufacturer
  - Issued a recall
  - Also threatened lawsuits
- Owner can
  - Go to an administrator web page
  - Enter the default credentials
  - Change to a new password



# 2018 Attacks

- Tech/Helpdesk Password Resets
  - Volume causes Techs to use defaults
- Default Router Password WebPages
- IoT Botnet Attacks Continuing



# Default Password Solutions

- Change Default Passwords
- Use Unique Passwords
- Use Alternative Authentication Mechanisms
- Force Default Password Changes
- Restrict Network Access
- Identify Affected Products
- Audits and Continuous Monitoring





# Solutions IoT

- Secure wireless network
  - Obscure name
  - Disable network guest access
  - Firewall
- Good password management
  - If possible
- Install a unified threat management appliance (UTM)
- Examine each IoT device you own



# Solutions IoT (Continued)

- Install security software wherever possible
- Check manufacturers' websites for firmware updates
- Pay attention to brands



“Those who don't know history are doomed to repeat it”

- Attributed to:

- Edmund Burke
- George Santayana
- Winston Churchill
- Jessie Ventura

- Applies to the default password conundrum

- Problem existed over 40 years ago
- Bigger than ever with IoT devices