IoT Threat Types

Dale Meredith
AUTHOR/TRAINER/SECURITY DUDE

@dalemeredith www.daledumbsitdown.com

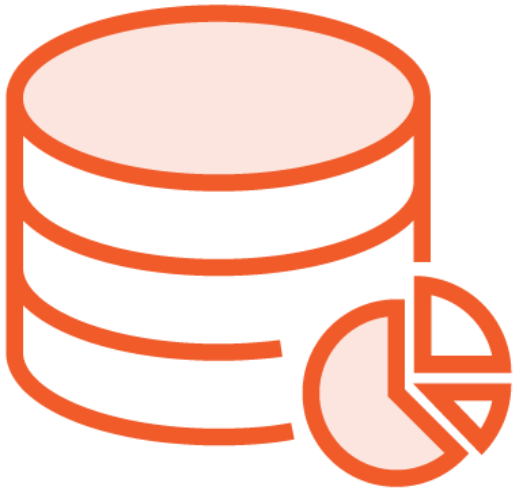
What We'll Cover

- Vulnerabilities and hurdles
- The massive attack surface
- Top 14 threats
- A case study: The Target Breach

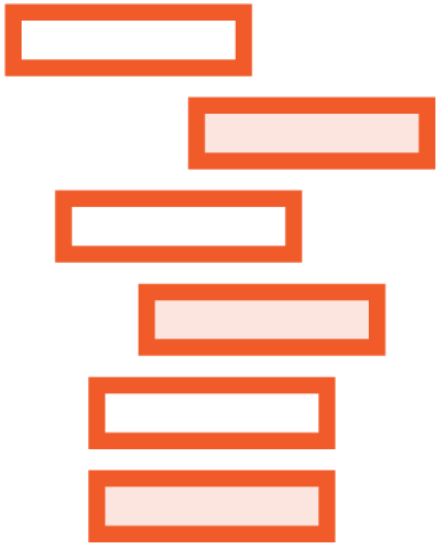
Vulnerabilities and Hurdles

The Issues

Data Value



Aggregation of Data



Integration

Oh yeah, Healthcare

The Culprits

Application

Mobile

Cloud

Network

OWASP's Top 10

- Insecure network services
- Authorization/ Authentication
- Insecure web interface
- Absence of encryption
- Physical security

OWASP's Top 10

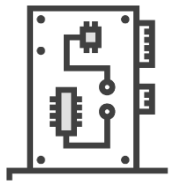
- Privacy issues
- Insecure mobile apps
- Cloud interfaces
- Configurability
- Firmware/ Software

The Massive Attack Surface

Did I Mention Massive?

Device memory

Ecosystem access control



Physical interfaces

Did I Mention Massive?

Web interface

Firmware

Network services

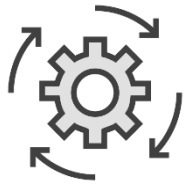
Did I Mention Massive?

Admin interfaces

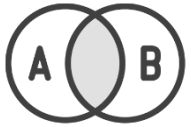
Data storage (local)

Cloud web interface

Did I Mention Massive?



Updating



3rd party backend APIs

Vendor backend APIs

Did I Mention Massive?

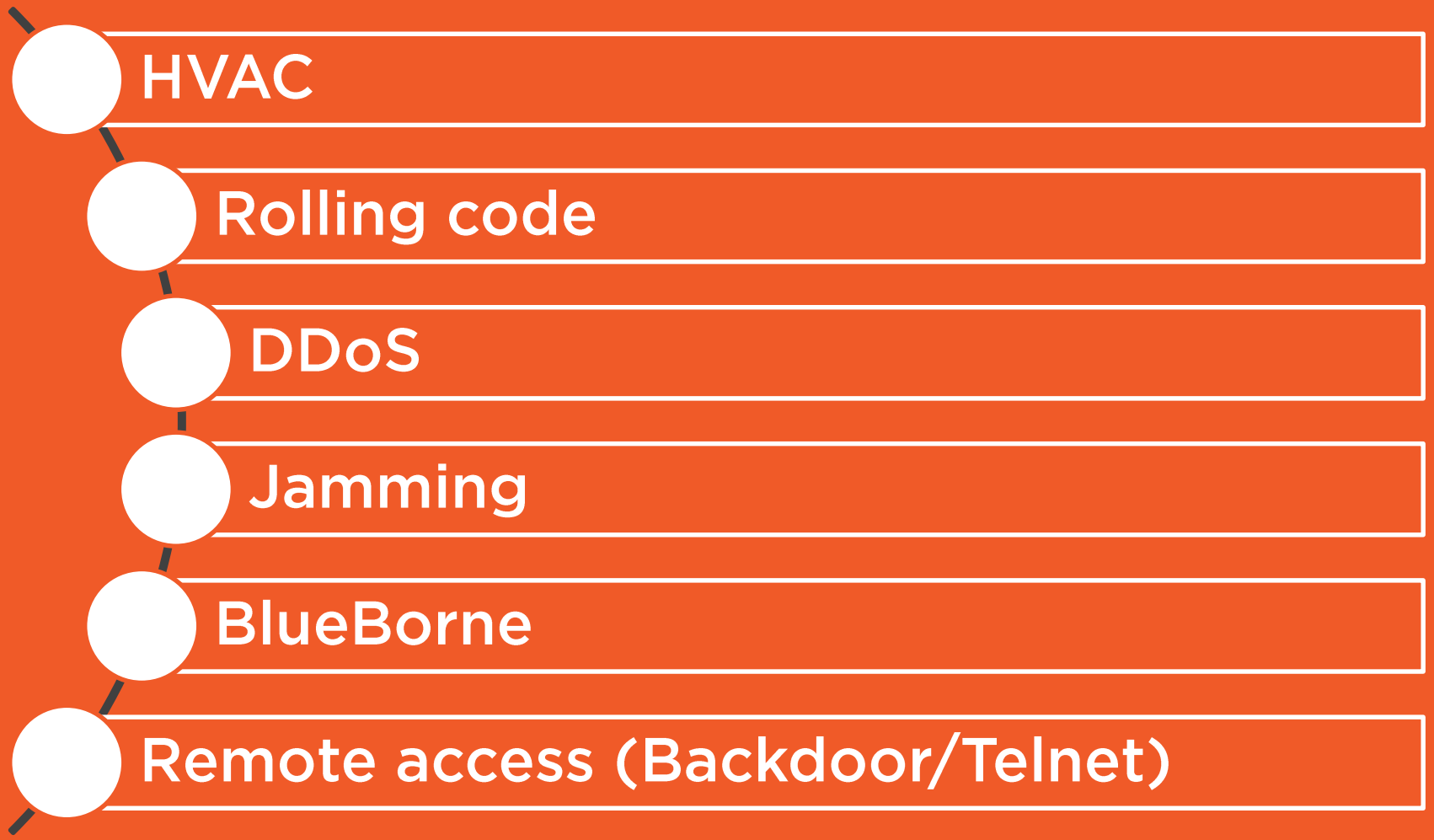
Communications within the ecosystem

Network traffic

Mobile apps

Our Top 14 Threats

Let The Attacks Being



Let The Attacks Being

- Exploit kits
- Man-in-the-middle
- Replay
- Sybil
- Forged device
- Ransomware
- Side channel

A Case Study: The Target Breach

The Target Is the Target

Google searches – results would have shown a vendor portal and vendors

Email malware sent to HVAC vendor

Access vendor portal - Pivot point

ID “misconfigured” systems

Install malware on POS systems via SCCM

The Target Is the Target

Used a ICMP tunnel to transfer data from POS to a compromised system

Default username/pw for BMC's Performance Assurance for Microsoft Servers product

FTP data to several "drop" locations worldwide

FireEye saw it, notified Target...No action

The Target Is the Target

$71M+

$61M+

40M cards

70M customers

80+ class action

4+ civil suits

The Target Is the Target

FTC investigation

DOJ investigation

USSS investigation

What We Talked About

- Vulnerabilities and hurdles
- The massive attack surface
- Top 14 threats
- A case study: The Target Breach