Defending Against Personal and Institutional Cyber Attacks

Gordon B. Agnew
University of Waterloo

Everyone who works here
Everyone who doesn't work here
klossner

" WE'VE NARROWED OUR SECURITY RISKS DOWN to THESE TWO GROUPS."

Why Cyber Attacks

- Increasingly, individuals and institutions are being subjected to cyber attacks
- What are attackers after?
  - – Personal medical information
    - Impersonation to order expensive drugs
  - – Financial gain

Attacks Against Hospitals

- Recently, a number of hospitals have been infected with ransomware
  - Hollywood Presbyterian Medical Centre
  - Baltimore’s Union Memorial Hospital
  - Methodist Hospital in Kentucky
  - Two Hospitals operated by Prime Healthcare in California
  - Ottawa

Attacks Against Hospitals

- Ransomware usually enters a system via *phishing* email attacks.
- An email is sent with an “innocent” looking attachment that contains the malware.
- Ransomware spreads through system encrypting data – attackers then demand a ransom to unlock the data (usually using anonymous bitcoin payments)

"We forgot to back up our files, so we're asking everyone to remember everything they've typed during the past 10 days."

How to Avoid Such Attacks

- Education!
  - Train system users to avoid phishing attacks
- Backup Regularly
  - IT personnel should establish a comprehensive backup program
- Keep systems patched and up to date

Wearable Devices

- We are seeing a large increase in the number and variety of wearable medical and fitness devices that can be accessed wirelessly
  – Heart rate monitors
  – Continuous glucose monitors
  – Temperature monitoring
  – Distance walked/run
  – Etc.
- Estimated to be $53 billion market worldwide and growing

Wearable Devices

- Some devices include gps tracking to provide accurate distance, speed, etc.
- This may be transferred to a device collection and analysis (iPhone, android, etc.)
- Many of these devices either have no security or it is very weak or the applications leak information.

Fitness Devices

- Top Vendors
  - FitBit
  - Apple
  - Xiaomi
  - Garmin
  - Samsung
- Most use Bluetooth to wirelessly communicate
- The data can be intercepted by an attacker

INFUSED 62.0mL
OR 62.0 mg
SILENCE
STOP
START
ABBOTT
GEMSTAR™
POWER
1
2
3
4
5
6
7
8

More Serious Attacks

- LifecarePCA is a drug infusion machine many hospitals use
- Two issues
  - The pumps access a drug library on the hospital’s network that contains patient data as well as drugs and dosage. It may be possible for an attacker gaining access to the network and alter the library
  - There is no authentication done for firmware updates
- FDA has issued warnings about security threats

IS-1
ST. JUDE MEDICAL
Sylmar, CA USA
VICTORY™ SR
5610 SSIR
S/N 1723182

More Serious Attacks

- “HOW DICK CHENEY TOOK HIS HEART OFFLINE TO THWART HACKERS”
- Some pacemakers have wireless interfaces
- In 2008, it was demonstrated that certain pacemakers could be hacked and be programmed to deliver fatal shocks

MiniMed
PARADIGM
B
ESC
ACT

More Serious Attacks

- **"Insulin pump hack delivers fatal dosage over the air"**
- A number of Medtronic insulin pumps have been subject to hacking
- In 2011, it was demonstrated that these pumps could be hacked and manipulated from over 30m away

Why is There a Problem

- In many cases, device manufacturers did not consider privacy of user data and security of the device to be important
- Security was added afterwards, homebrew encryption was used to reduce power requirements and cost

What is the Future?

- People are much more aware of the need for data privacy and device security
- Device manufacturers are now incorporating security mechanisms into their products from the design stage
- Standards are evolving for wireless medical devices
- The next frontier – The Internet of Things

The Next Frontier
The Internet of Things

IoT

- Originally designed to automate simple devices
  - Lights
  - Heat
- New uses include home security
- Protocols were never really intended to provide high levels of security – home security systems can be jammed, door locks opened remotely
- New protocols are being developed but current devices are generally vulnerable