CERIAS

The Center for Education and Research in Information Assurance and Security

Malware in Medical Devices

Susan Fowler, Dr. Samuel Liles

CIT Forensics Lab

Abstract

Health care facilities are increasingly adopting computers and medical devices into patient care regimens and therapies. Medical devices have evolved to become popular for many purposes, including prolonged managed care including implantable medical devices. Wireless communications are becoming popular for these IMDs as well as for networking medical devices in a clinical setting. Along with these progressions in technology, security and privacy must be considered to ensure patient privacy and safety. Malware can be introduced in many of the same ways traditional computer systems suffer compromises, with wireless technology compounding these vulnerabilities. Regulations and practices must recognize these threats to security, availability and privacy to both health care entities and patients.

Keywords: Medical device, malware, information security

Research Question

What is the pervasiveness of malware in medical devices and are medical facilities prepared and equipped to deal with the threat

Previous Work

Medical devices becoming more prevalent in therapies (Yeo, 2010)

No framework for capturing security related incidents in medical devices (Fu & Blum, 2013)

Counterfeit update vulnerabilities (Hanna et al, 2011)

Security design goals (Halperin et al, 2009)

Methodology

Government statistics

Academic sources

Prevalence of the issue

25 million people have an implantable medical device

How secure?

1.2 million adverse attacks 2006-2011

72% of malicious attacks target hospitals

No nationally recognized system for reporting incidents

Federal Regulations and Guidelines

FDA

NIST

Department of Homeland Security

Integrity and Availability

Dependency on unsupported platforms

Mismatch in device system cycles

Use of off the shelf platforms

Lack of timely patches

FDA constricts patching capabilities

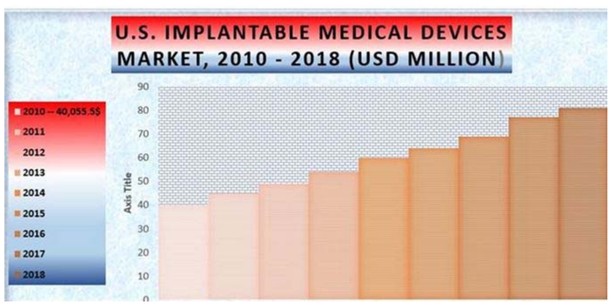
No reliable framework for medical device security

Access Control Issues

Performance reduction

Preference of older software

After market security risks



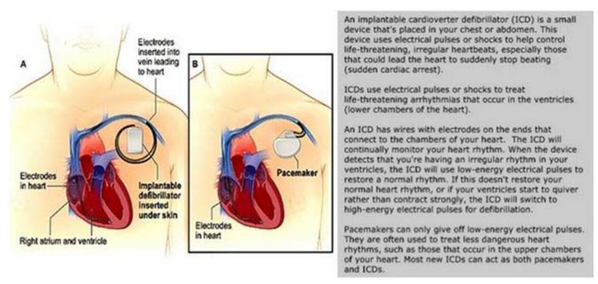
Wired vs. Wireless

Implantable devices converting to wireless capabilities

System and network security considerations

Software security considerations

Software susceptible to rapid change



History of Medical Devices

Jay Radcliffe at IBM alters a insulin pump

Pacemakers/ICD capable of full radio frequency

Barnaby Jack demonstrated how to hack a pacemaker to send electronic shocks

He accessed servers that engineer the software, enabling him to upload viruses

Medical device software is a new area of study

Unsecure Medical Devices Future Issues (What If)		
Threat	**Target**	**Impact**
Private medical history released to public	Political or candidate for office	Private information swings public opinion of a potential office holder
Attack of terrorism on medical infrastructure	Medical device within hospital Infrastructure	Loss of confidence and fear causing monetary damage
Information altered to implicate person in crime	Medical device implanted	Personal loss, time, money, reputation
Identity Theft	Personal, to get treatment	Treatments given to individual/ Capital for Hospital
Identity Theft/criminal	Personal, to plant information	Respect, integrity, indictment
Black market for updated devices	Individuals, insurance,	Untrusted devices in hospital system
Unreliable devices/software issues	Clients, insurance	Service, integrity

Potential Safeguards

Heartbeat rhythms act as a biometric detector

Google glass

Conclusion

Cyber security at the development level

Encourage users to report suspected or recognized security incidents

Ensure device lifecycles match software installed

Control human factor risks

Cryptographically secure system updates

Defenses and updates have to be weighed with their risk to the patient

CERIAS®

PURDUE UNIVERSITY