IoT: Hackers, Attack Anatomy & Security Trends

By Ted Harrington, Executive Partner, Independent Security Evaluators (ISE)

Submitted for Speaker Consideration

Abstract

As devices become increasingly connected, attacks against the Internet of Things are rampantly increasing. Some devices are purpose-built to be connected, while others were built for an analogue world and retrofitted to meet demand for connectivity. Both types introduce potentially catastrophic security implications if designed or implemented improperly. As malicious hackers advance their techniques at a staggering pace, often rendering current defense tactics obsolete, so too must security practitioners obsess over deploying progressive techniques. Presented by the elite organization of white hat hackers most widely known for being first to break the iPhone and more recently for their discovery of the vulnerability epidemic in wireless routers that connect many IoT devices, this session will analyze the anatomies of real world attacks against high profile systems, ranging from the well known Target breach, to Texas Instruments RFID, to Apple products, and more. It will extract lessons from these attack anatomies to provide a framework to account for these modern attackers, articulate context to the evolving IoT industry, and supply attendees with key takeaways, including immediately actionable guidance.

Goals & Presentation Perspective

The presentation will attempt to resonate with the audience by exploring issues from their perspective (i.e., that of business executives and IT managers responsible for security). We will utilize case studies from our work to highlight decision-points, such as selected communication protocols, wherein we will analyze the advantages and disadvantages of various decisions on the impact of system security. The goal is to provide valuable guidance to both IT executives who are fluent in the new digital era as well as to those who are struggling to adapt to the ferocious pace at which technology is changing.

I. Discipline Division: Security Separated from Functionality.

Where these conflicting functions have traditionally existed within the same IT groups, progressive enterprises are evolving to separate *security* and *functionality* into distinct operations. These roles conflict, and when a person/department is responsible for both, *functionality* generally prevails, thereby leaving the enterprise insecure. This trend towards discipline division is new or not yet existent in most enterprises, and highlights a movement towards more secure network environments.

II. Perspective Matters: White Box vs. Black Box.

To improve the security posture of digital technologies, progressive organizations engage third party security experts to assess risk and provide hardening guidance. The most suitable approach is typically *white box vulnerability assessment*. However, confusion about different security approaches has led executives and IT managers to commonly request the notably ineffective approach known as *black box penetration testing*. Most executives may be surprised to discover that this approach actually undermines the very risk assessment objectives they seek to achieve. *This trend highlights a movement towards less effective risk calculation.*

III. Defense Priorities: Secure Assets, not Just Perimeters.

Traditionally, companies have focused on hardening perimeter defenses: firewalls, routers, antivirus, etc. Much less focus has been paid to internal defenses. Modern attacks circumvent these defenses, and many attacks originate from within trusted boundaries. Progressive enterprises are making a paradigm shift in their approach to focus on securing assets, and not just hardening the perimeter. This security principle is known as *defense-in-depth*. This trend highlights a movement towards assuming a breach has already or will soon occur, and implementing fail-safes accordingly.

IV. Timing Security: Build It In, Not Bolt It On.

Due to the ferocious timelines most development teams are under, focused efforts on mission critical development milestones often take precedence over anything to be addressed later in the process. For this reason, security review is often relegated to a last minute consideration. Progressive enterprises and software development teams integrate security in to the process at the Design stages and during the Agile process, rather than during or after Deployment. It has been shown to be substantially more expensive to address security issues found after Deployment than those issues identified in Design, as security is a requirement, not a feature. This trend highlights a movement towards more efficient, cost-effective security development practices.

V. Procedural Duration: Security as an Ongoing Process.

As technologies evolve, security posture migrates. In that vein, security should be engaged along the same timelines. Ongoing guidance is showing strong results in defending against constantly evolving attack methods. Development is never complete, and thus if not part of the iterative development process, security may become delayed indefinitely. This trend highlights the role of security in the development cycle evolving towards a more ongoing, granular approach.

About the Presenter

Ted Harrington drives thought leadership initiatives for Independent Security Evaluators, the elite organization of security researchers and consultants widely known for being the first company to hack the iPhone. He is a sought-after speaker, presenting at high-profile conferences in a range of industries, including for the CyberTech Securing IoT, National Association of Broadcasters (NAB), Content Delivery & Security Association (CDSA), Information Systems Audit and Controls Association (ISACA), and others.

Mr. Harrington holds several special appointments, including to the University of Southern California. He was recently named a *40 Under 40* executive by SD Metro Magazine, where he was not only one of the youngest inductees in the class but was also the only honoree from the field of information security. He holds a bachelors degree from Georgetown University.

About ISE

Founded in 2005 out of the PhD program at the esteemed Johns Hopkins' Information Security Institute, ISE is a sophisticated security consulting firm dedicated to aggressive defense strategies through advanced science. This select team of hackers, computer scientists, reverse engineers, and cryptographers helps enterprises defend against sophisticated hackers by utilizing a perspective typically perpetrated by the adversary.

ISE is most commonly recognized for being the first company to exploit the iPhone[1], an achievement that garnered international attention. Other high profile compromises include ExxonMobil SpeedPass, Texas Instruments RFID, Diebold eVoting Machines, and numerous others. ISE's most recent research discovered systemic issues in wireless routers[2], network attached storage[3], and web browsers[4]. ISE is the organizer DEF CON's first-ever router hacking competition *SOHOpelessly Broken*, named after the seminal research of the same name.

---

[1] http://www.nytimes.com/2007/07/23/technology/23iphone.html?_r=2&
[2] http://securityevaluators.com/content/case-studies/routers/soho_router_hacks.jsp
[3] http://www.infoworld.com/d/security/network-attached-storage-devices-more-vulnerable-home-routers-247875
[4] http://securityevaluators.com/content/case-studies/caching/index.jsp