SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- Suits and Spooks

Security Experts:

WRITE FOR US

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe (Free)
- Security White Papers
- ICS Cyber Security Conference
- Contact Us

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - White Papers
  - Desktop Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
  - Whitepapers
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
  - Whitepapers
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - White Papers
  - Network Security
  - Application Security
- Management & Strategy

Risk Management
Security Architecture
Disaster Recovery
Incident Management
Training & Certification
Critical Infrastructure
Home › Network Security

IoT: The Security Risk Iceberg

By Torsten George on September 23, 2015

Share 8 G+1 0 Tweet 49 Recommend 1 RSS

While politicians and security experts are constantly warning about the risk of cyber-attacks, they rarely, if ever, mention the risks associated with the Internet of Things (IoT). They should. Global connectivity between all devices creates significant security concerns. Recent reports of hackers being able to remotely control cars illustrate the immense risks posed by IoT. This raises questions regarding current security risk management practices and illustrates the challenges that are being created by IoT's all-in-one connectivity.

What is IoT anyway? According to analyst firm Gartner, "IoT is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment". Nowadays many devices have embedded operating systems and are connected to the Internet, which introduces a board range of new opportunities for consumers and businesses alike. Gartner predicts that by 2020 there will be over 26 billion connected devices, while other analysts believe the number will exceed 100 billion.

There are many applications of IoT, ranging from a house alarm system providing status alerts to a smartphone, smartwatches collecting health data and sharing it with doctors, vehicles accessing calendar data to pre-calculate the best route to take the driver to an offsite meeting, a wake up alarm triggering the coffee machine to prepare a dark roast just minutes it wakes the user, a refrigerator reminding the owner to purchase grocery items, or office equipment automatically re-ordering supplies when they run low. On a macro-level, smart city applications such as smart lighting and smart parking, would allow us to reduce waste and improve efficiency for things such as energy use. IoT provides endless opportunities and interactions, many of which we can't even imagine yet.

The IoT market is still in its infancy, but is being driven by high expectations built around offering consumers a more convenient life style. Meanwhile, it promises to open up new markets for businesses by providing vast amounts of information on customer buying habits, which can be leveraged to drive further sales.

However, there is also a darker side to IoT, related to security and privacy. A good example is the recent case of hackers taking control of a car and crashing it into a ditch by remotely breaking into its dashboard computer from 10 miles away. That this is not an isolated incident was documented in a study by PT&C|LWG Forensic Consulting Services, which outlined that many other car makers' were susceptible to being hacked. This is just one illustration of the tip of the iceberg when it comes to IoT's security risks. Unlike traditional cyber-attacks, IoT incidents are not limited to extracting information; instead they can be used to cause physical harm and exploited by statesponsored cyber-attackers to wreak havoc.

Ultimately, IoT opens up companies all over the world to more security threats. According to Robert Bigman, former CISO at the Central Intelligence Agency (CIA), IoT devices that manage personal health and safety systems will become the next ransom-ware gold mine. Like they have for the Bring-Your-Own-Device (BYOD) phenomenon, businesses need to adapt their risk management practices and broaden the scope of risk assessments to include all connected devices. If an employee's smartwatch can be leveraged to spy on the corporate's WiFi passwords, the watch suddenly falls into the scope of an organization's risk assessment. In this context, one of the leading challenges for organizations will be how to store, track, analyze, and make sense of the vast amounts of data generated by including IoT in the risk assessment process. Emerging big data risk management technologies can assist here.

To complicate matters, the development of IoT products preceded the creation of a common security framework or standard. In the case of many IoT products, security is an afterthought. The only reasonable solution to address the lack of security in IoT devices is for new standards and government regulations to be established that require the use of trusted networks and operating systems.

While it is encouraging to see several initiatives (e.g., Cloud Security Alliance, Open Interconnect Consortium) working to create frameworks to secure IoT ecosystems, an accepted standard will be needed to ensure the interoperability required to achieve this goal. Until then, IoT vendors need to incorporate security at the design phase of products to make them less of a threat when connected to networks. In addition, they need to consider early on what regulations devices will have to comply with so those requirements can be baked in and not added later when they would be less effective. Finally, device communication channels should conform to standards-friendly hub-and-spoke networking protocols, which are less vulnerable to attacks.

Time will tell if the IoT vendor community can come together to create a common security framework that helps shrink the security risk iceberg and minimize the risk of cyber-attacks.

Related: Learn About IoT Security at the 2015 ICS Cyber Security Conference

SECURITYWEEK BRIEFING Be Informed. Subscribe Free

Share 8 G+1 0 Tweet 49 Recommend 15 RSS

Torsten George is Vice President of Worldwide Marketing and Products at integrated risk management software vendor Agiliance. With over 20 years of global information security experience, Torsten frequently presents and provides commentary on compliance and security risk management strategies, data breaches, cyber security, and incident response best practices. Torsten has held executive roles with ActivIdentity (now part of HID Global), Digital Link, and Everdream Corporation (now part of Dell). He holds a Ph.D. in Economics and an M.B.A.

Previous Columns by Torsten George:
IoT: The Security Risk Iceberg
The Real Inhibitors of Risk Management
Smoke and Mirrors: Cyber Security Insurance
Stepping Up Security Risk Management Practices
Following the Regulatory Beat: Continuous Compliance

Download Free Security Resources from the SecurityWeek White Paper Library

sponsored links

2015 ICS Cyber Security Conference: Oct. 26-29 - Atlanta, Ga

WEBCAST: Best Practices for Privileged Identity Management (6/30/15)

View Our Library of on Demand Security Webcasts

Tags:
INDUSTRY INSIGHTS Network Security Risk Management Vulnerabilities

0 Comments SecurityWeek provides information security news and analysis. 1 Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

ALSO ON **SECURITYWEEK PROVIDES INFORMATION SECURITY NEWS AND ANALYSIS.** WHAT'S THIS?

Default WSUS Configuration Puts Organizations at Risk: Researchers

1 comment • a month ago

Ian Crowl — we have set up SSL from our clients to the wsus server. but this seems as if the connection from Microsoft Updates …

Industry Reactions to Oracle CSO Rant: Feedback Friday

1 comment • a month ago

BorateBomber — There is that old cantrip, "Trust, but Verify". Her post broke that rule.

Tor Increasingly Used by Malicious Actors: IBM

1 comment • a month ago

Sean — As it should be, that's what it is well matched for.

Snowden Attacks Russia Rights Curbs, Would Prefer to Go Home

5 comments • 17 days ago

Minh Ng — I prefer Snowden being execute in front of people or suffer life in prison for his crime against his own country. The things …

Subscribe Add Disqus to your site Privacy

Search

Subscribe to SecurityWeek

Enter Your Email Address Subscribe

Most Recent Most Read

- US Says 5.6 Million Fingerprints Stolen in Breach
- HP Launches Secure Enterprise Printers
- Firefox 41 Patches Critical Vulnerabilities
- Google Drive Gets Security Enhancements
- IoT: The Security Risk Iceberg
- Large Number of iOS Apps Infected by XcodeGhost
- Forbes Hit by Malvertising Campaign: FireEye
- Xi Jinping: China Defender of Cybersecurity
- Dell Enhances Enterprise IAM Solution
- Android Malware Possibly Infects 1 Million Devices via Google Play

Popular Topics

Information Security News
IT Security News
Risk Management
Cybercrime
Cloud Security
Application Security
Smart Device Security

Security Community

- IT Security Newsletters
- IT Security White Papers
- Suits and Spooks
- ICS Cyber Security Conference
- CISO Forum
- InfosecIsland.Com

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Cyber Weapon Discussion Group
- RSS Feed
- Submit Tip
- Security Intelligence Group

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us

Wired Business Media

Copyright © 2015 Wired Business Media. All Rights Reserved. Privacy Policy | Terms of Use