6 Hot Internet of Things (IoT) Security Technologies

Internet of Things (IoT) security breaches have been dominating the headlines lately. WikiLeaks's trove of CIA documents revealed that internet-connected televisions can be used to secretly record conversations. Trump's advisor Kellyanne Conway believes that microwave ovens can spy on you—maybe she was referring to microwave cameras which indeed can be used for surveillance. And don't delude yourself that you are immune to IoT attacks, with 96% of security professionals responding to a new survey expecting an increase in IoT breaches this year.

Even if you personally don't suffer the consequences of the sub-par security of the IoT, your connected gadgets may well be unwittingly cooperating with criminals. Last October, Internet service provider Dyn came under an attack that disrupted access to popular websites. The cybercriminals who initiated the attack managed to commandeer a large number of internet-connected devices (mostly DVRs and cameras) to serve as their helpers. As a result, cybersecurity expert Bruce Schneier has called for government regulation of the IoT, concluding that both IoT manufacturers and their customers don't care about the security of the 8.4 billion internet-connected devices in current use.

Whether because of government regulation or good old-fashioned self-interest, we can expect increased investment in IoT security technologies. In its recently-released TechRadar report for security and risk professionals, Forrester Research discusses the outlook for the 13 most relevant and important IoT security technologies, warning that "there is no single, magic security bullet that can easily fix all IoT security issues."

Based on Forrester's analysis, here's my list of the 6 hottest technologies for IoT security:

1. **IoT network security**: Protecting and securing the network connecting IoT devices to back-end systems on the internet. IoT network security is a bit more challenging than traditional network security because there is a wider range of communication protocols, standards, and device capabilities, all of which pose significant issues and increased complexity. Key capabilities include traditional endpoint security features such as antivirus and antimalware as well as other features such as firewalls and intrusion prevention and detection systems. Sample vendors: Bayshore Networks, Cisco, Darktrace, and Senrio.
2. **IoT authentication**: Providing the ability for users to authenticate an IoT device, including managing multiple users of a single device (such as a connected car), ranging from simple static password/pins to more robust authentication mechanisms such as two-factor authentication, digital certificates and biometrics. Unlike most enterprise networks where the authentication processes involve a human being entering a credential, many IoT authentication scenarios (such as embedded sensors) are machine-to-machine based without any human intervention. Sample vendors: Baimos Technologies, Covisint, Device Authority, Entrust Datacard, and Gemalto.

3. **IoT encryption**: Encrypting data at rest and in transit between IoT edge devices and back-end systems using standard cryptographic algorithms, helping maintain data integrity and preventing data sniffing by hackers. The wide range of IoT devices and hardware profiles limits the ability to have standard encryption processes and protocols. Moreover, all IoT encryption must be accompanied by equivalent full encryption key lifecycle management processes, since poor key management will reduce overall security. Sample vendors: Cisco, Entrust Datacard, Gemalto, HPE, Lynx Software Technologies, and Symantec.
4. **IoT PKI**: Providing complete X.509 digital certificate and cryptographic key and life-cycle capabilities, including public/private key generation, distribution, management, and revocation. The hardware specs for some IoT devices may limit or prevent their ability to utilize PKI. Digital certificates can be securely loaded onto IoT devices at the time of manufacture and then activated/enabled by third-party PKI software suites; the certificates could also be installed post-manufacture. Sample vendors: DigiCert, Entrust Datacard, Gemalto, HPE, Symantec, and WISeKey.
5. **IoT security analytics**: Collecting, aggregating, monitoring, and normalizing data from IoT devices and providing actionable reporting and alerting on specific activities or when activities fall outside established policies. These solutions are starting to add sophisticated machine learning, artificial intelligence, and big data techniques to provide more predictive modeling and anomaly detection (and reduce the number of false positives), but these capabilities are still emerging. IoT security analytics will increasingly be required to detect IoT-specific attacks and intrusions that are not identified by traditional network security solutions such as firewalls. Sample vendors: Cisco, Indegy, Kaspersky Lab, SAP, and Senrio. (See also my post regarding Aperio Systems)
6. **IoT API security**: Providing the ability to authenticate and authorize data movement between IoT devices, back-end systems, and applications using documented REST-based APIs. API security will be essential for protecting the integrity of data transiting between edge devices and back-end systems to ensure that only authorized devices, developers, and apps are communicating with APIs as well as detecting potential threats and attacks against specific APIs. Sample vendors: Akana, Apigee/Google, Axway, CA Technologies, Mashery/TIBCO, MuleSoft, and WS02.

Note that Forrester did not identify any technologies in the "creation" stage. It says: "The continued evolution of IoT-specific security threats will undoubtedly drive innovation in this space, so expect more new IoT-specific security technologies to appear in the creation phase in the near future, many of which may align around vertical- and industry-specific use cases such as connected medical devices or industrial applications."

Forrester lists the following challenges to achieving a secure IoT: Many IoT devices lack basic security requirements; There is a plethora of IoT standards and protocols, which creates security blind spots; The scale and scope of IoT deployments hinder visibility into security incidents; There is a lack of clarity of responsibility regarding privacy and security.

"The Dyn attack was likely just the start," says Forrester, "so [we] can expect further attacks that leverage insecure IoT devices in the coming months and years." Indeed, Gartner placed security at the top of its list of top 10 IoT technologies for 2017 and 2018, saying "IoT security will be

complicated by the fact that many ‘things’ use simple processors and operating systems that may not support sophisticated security approaches.”

It’s complicated when simple things connect to become a vast network that reaches everywhere. Forrester makes the following observations and recommendations: IoT security requires an end-to-end approach; Encryption is an absolute must; IoT security scenarios place a premium on scalability (dealing with the sheer number of devices); Security analytics will play a significant role in IoT security solutions; IoT standards are important catalysts but still need time to mature.

Concludes Forrester: "It’s imperative for today’s digital businesses to balance the business benefits that IoT-connected products can deliver with the recognition that these same devices have become an attractive attack plane for hackers and cybercriminals seeking to cause disruption and exfiltrate sensitive data.”