VIEWING CONNECTED THINGS THROUGH A SECURITY LENS

Back in 1999, Kevin Ashton, while working as an Assistant Brand Manager for Procter & Gamble, wondered why a certain cosmetic product always showed "out of stock" on grocery store shelves. This led him on to think of the possibility of a wireless network that could snatch data off a tiny "radio-enabled" chip on, say, a lipstick pack from a warehouse and keep store managers better informed about their inventory. He soon coined the term "Internet of Things" (IoT) and made a presentation about embedding everyday objects with sensors that were powered by the Internet. Nearly two decades on, human kind hasn't even begun utilizing IoT to its fullest potential, mainly due to two challenges – privacy and security. Technology has grown to gain insights from data in real time for business outcomes, yet human beings are apprehensive over breach of security and concerns over confidentiality, integrity, availability and most importantly, the abusive control of personal data. (Trust remains the business currency for the new-age consumer.)

IoT devices have permeated industries, from consumer products to manufacturing processes and public services; however, the banking domain remains at the cusp of influencing consumer financial behavior today. Who would have imagined the surge of the Quantified Self Movement fuelled by the IoT and wearables industry, collecting raw data continually on various vital parameters and churning them into meaningful insights related to consumer health and fitness, insurance claims processing or flexible interest rates? Many more autonomous banking related IoT use cases have been identified since, such as a cars making payments on user authorization or underwriting decisions influenced by IoT monitoring.

Cross-disciplinary functions seamlessly blend in an IoT-connected ecosystem. It is no paradox to state that the next big thing will actually be multiple, small heterogeneous "powered-things" without a visible user interface, that can handshake data and create a sensor-driven marketplace to drive decisions. Several vendors will offer devices at lower prices, driving the market; however, security and privacy discipline by IoT manufacturers and integrators will have to instil confidence and promote adoption of these ubiquitous devices in mass-market and niche segments. Understanding the threats involved should begin with a breadth- and depth-first approach that can create a security lock as demonstrated in Figure 1.

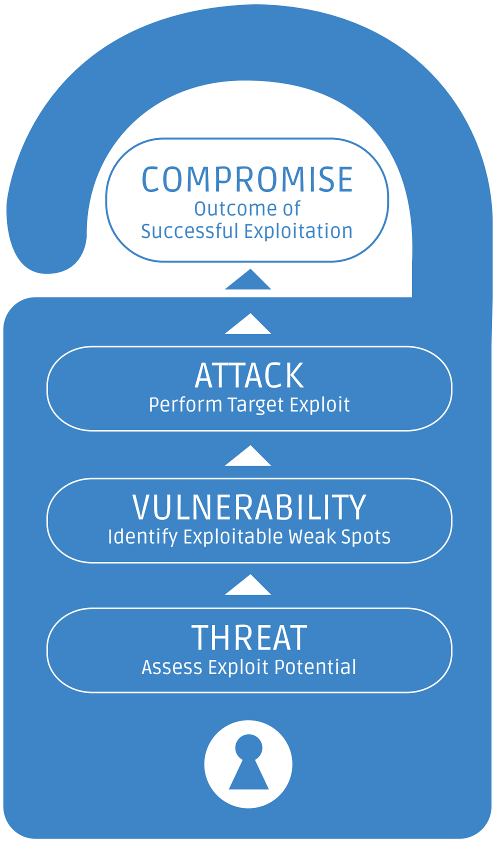

Figure 1: Unlocking the anatomy of an attack

Banking IoT Use Cases

Corporate Lending – Loan Risk Avoidance

In the corporate lending business, there are multiple functions that qualify for automation such as loan underwriting, reviews and audits, risk analysis and foreclosure avoidance, which are all cost centers for banks. Tech-savvy banks are looking for ways to avoid loan default scenarios (wherein unpaid loan amounts are written off in balance sheets). This is an ideal scenario for IoT that can result in a bank receiving an alert in advance about its Non-Performing Assets. Imagine an industrial scenario where motion, position and GPS sensors are embedded in machinery on which the bank has a lien. Banks can receive alerts indicating stalled industrial production or instances of a plant heading for a shutdown due to being unused. (In some cases, the recipient of the loan may have even planned a resale of the machinery.)

Geo-tagged data can perform risk analysis and stock audit reviews

IT IS NO PARADOX TO STATE THAT THE NEXT BIG THING WILL ACTUALLY BE MULTIPLE, SMALL HETEROGENEOUS "POWERED-THINGS" WITHOUT A VISIBLE USER INTERFACE, THAT CAN HANDSHAKE DATA AND CREATE A SENSOR-DRIVEN MARKETPLACE TO DRIVE DECISIONS.

at scheduled intervals. Movement of stocks hypothecated to a bank can be tracked and credit risk reduced. The purpose of the loan, date of sanction and information about usage can be corroborated to establish the credibility of the customer and their credit score. This in turn can flag off anomalies related to whether a portion of the entire loan amount sanctioned was diverted for unauthorized or fraudulent businesses, or even into tax havens. The system itself can be made to initiate loan instalment payments at periodic intervals with user authorization. Pervasive monitoring can spot financial stress moments at the borrower's end and help with contingency planning.

A question to be asked is whether customers can fool an IoT system by physically tampering with its sensors or intercepting and manipulating them through passive modes, such as scamming with sound waves to feed 'fake' data that can in turn present a scenario where a machine is seeming to be used continuously even when industrial production may have stalled.

Surveillance via Chip-enabled IoT Devices

Possessing a SIM Card is a passport to the land of IoT. There are numerous use cases where SIM cards can be embedded into everyday objects and transformed into IoT devices. Tomorrow, a button, a clip, a binder, a phone cover, a toy, any accessory, gadget or even any part of home decor can be embedded with a chip.

SIM swap scenarios are indicators of a change in ownership of the device, and even fraud. To counter such activities, many banks are experimenting with wafer-thin films stuck onto SIM cards. The film will install a SIM Tool Kit (STK)-based app, which can be accessed on any mobile even when there is no internet connectivity. Now, imagine this mobile device connected to a wallet that can be dynamically loaded and opened for remote provisioning. SIM cards can come with multi-operator support for enhanced resilience to network outages.

Real-time detection of a SIM swap can block fraudulent use without the need for additional authorization. SIM surveillance can spot users who have evaded loan payments and absconded. But, what happens if the SIM card is cloned? What if one access endpoint is compromised, or the server gets hacked through impersonation and is taken over by a rogue command-and-control center?

Securing in-car Payments with Transaction Authorization across Trust Boundaries

Imagine a common use case of in-car payments at gas stations, parking bays, convenience stores and toll booths. Integration of tamper-proof hardware such as NFCs, embedded secure elements and EMV chips enable cars to make payments by themselves.

A very common attack vector is to encode null bytes into transaction messages that are passed as strings that can get access to system files and resources. What if someone sent a malicious command that took control of the car's bootstrap function and exposed secret keys used for signing the transaction? For an IoT service ecosystem of connected cars, the critical recommendation for a secure endpoint architecture is to implement a trusted computing

WHEN DATA FROM IOT DEVICES IN CONNECTED CAR ECOSYSTEMS ARE TAMPERED WITH, THERE IS A STRONG LIKELIHOOD OF INSURANCE COMPANIES FAILING TO CORROBORATE SENSOR DATA WITH CLAIM REQUESTS.

base to prevent tampering of an application image during Over-The-Air (OTA) firmware updates. It is even more important to establish trust boundaries for separate administrative tasks that can be exclusively accessible with controlled privileges and authorization. Sometimes, car manufacturers can inadvertently expose device identifiers by printing them on the dashboard or etching them on glass windows, leading to metadata harvesting. This could lead to theft of the car or create a loophole in the system, causing unauthorized entry. When data from IoT devices in connected car ecosystems are tampered with, there is a strong likelihood of insurance companies failing to corroborate sensor data with claim requests. Even unsecured Wi-Fi and hotspots in a chain can make so-called secure card payments using tokenization possible, instead of actual cardholder data.

Perimeter Surveillance in Sensitive Environments

In enterprise banking, cash vaults can be installed with IoT sensors to track money movement in a day, including gatekeeper activities. Insider fraud and intrusion can be limited with such perimeter surveillance.

There are several use cases wherein users can hook up IFTTT (IF This Then That) APIs to create automated recipes. Figure 2 demonstrates that the scale of the security risk is as vast as the connections between the Web, mobile, API, cloud, network, data, hardware components, wearables and devices converge. When all of these come together as a chain, albeit a weak one, they can jeopardize the entire system and its participants.

Emerging Focus on IoT Security

Top on the security list is the need to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications, and to address new challenges such as impersonating "things" or denial-of-sleep attacks that can drain batteries. Common attacks on IoT include:

1. Denial of Service attacks: Impairs applications, systems and networks by exhausting resources.

2. Malware: Malicious code that interferes with confidentiality, integrity and availability of victim's data. Examples: Trojan, ransomware, virus, worms, Trojan Horses, logic bombs.

3. Distributed Denial-of-Service (DoS) attacks: Variant of DoS that use bots and distributed hosts targeting a victim's applications, systems and networks.

4. SQL Injection: Type of database attack trying to lead to unauthorized disclosure of sensitive information via open-ended query constructions.

5. Zero-day Exploit: Represents the window available to an attacker until public disclosure of a security vulnerability.

6. Wiretapping: Without altering information, monitoring or listening to data transmitted over a communication link that can expose sensitive information such as passwords (in clear-text).

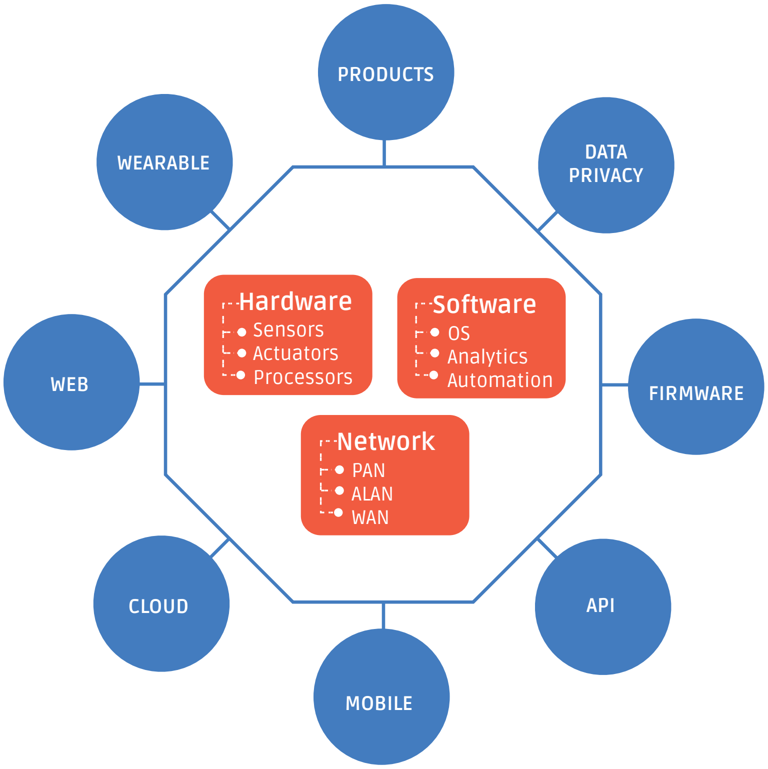

Figure 2: The Scale of Security Risk in an IoT ecosystem

7. War Diving: Use of powerful antennas to search for unsecured wireless networks, as in smart cities, distributed grids or connected-car networks.

The IoT Landscape viewed through a Security Lens

Given the ubiquity of technology and cheap devices available, there is a need for IoT watchdogs to define guidelines to include security as a feature for device/product manufacturers, platform integrators and developers so that the paranoid end consumer of IoT need not be worried about the hijacking of personal data. *(Please refer Open Web Application Security Project (OWASP)'s draft on IoT Attack Surface Areas [4] to understand IoT-driven security challenges.)*

Evolving IoT Security Standards

Several engineers and technologists in working groups have helped evolve security related to the Internet of Things (IoT) and made privacy recommendations; and, commendable among these include BITAG, OWASP, NISTGSM Alliance, IoT Security Foundation IoT Security Foundation, Industrial Internet Consortium and the Cloud Security Alliance.

IoT Device manufacturers are the custodians of equipment data. Operational data could be raw (JSON/XML) or processed (insights from analytics) inputs from consumers. This data should be protected as per the terms of the license agreement of an IoT contract, and should include who owns what, rights of the licensor and licensee, territorial rights and subjects, rights to sublicense terms, and exclusivity of contractual terms.

From an IoT endpoint device perspective, devices need to possess the following characteristics: low cost and power consumption, longer life and physically accessible endpoints.

OWASP IoT Security Principles

Developing cutting edge security in IoT platforms involves ingraining confidentiality—integrity-availability elements into the compliance class in products/services and ensuring that manufacturers get their products/services "certified" with prominent marks, seals and icons displayed to the public, and easily understood by the consumer. OWASP's top 10 IoT vulnerabilities have been available in the public domain since 2014. Every product/ service in the IoT system is included for certification and quality assessment. A product/service that fails to comply is declassified and revoked from the market. There is a need to establish procedures for delivery and receipt of personalized security credentials for the devices themselves. (Please refer to chart 1 that explains the OWASP's Principles of IoT Security that need to be considered by every component manufacturer in the IoT value chain.)

Chart 1: OWASP's principles of IoT Security

S No	IoT Security Principles	What they mean
1	Assume a Hostile Edge	Pervasive Monitoring is a threat; assume that attackers always have the edge.
2	Test for Scale	Assume DoS attacks; availability is at stake. Even simple bootstrapping needs to be secure proof.
3	Internet of Lies	Imagine the effect of "Chinese whispers". Misinformation can be be convincing.
4	Exploit Autonomy	Though, this may be the end of human monotony, powered devices now have the full discretion to make decisions on their own.
5	Expect Isolation	Whether connected or disconnected, security as a feature must never diminish under isolation. Devices should function even if the Internet is disrupted. Unplug and quarantine devices, if found infected.
6	Protect Uniformly	Data and metadata are at risk. Protect data in transit, at rest, and in use, always. Every component needs a unique identifier.
7	Encryption is Tricky	Choice of cipher suites, algorithms, key sizes and management throughout the lifecycle have to be considered.
8	System Hardening	There is a need to establish minimum viable attack surfaces; disable unknown ports, unnecessary services; and, delete default passwords.
9	Limit what you can	Deny by default, restrict usage and limit unwanted exposure that is subject to abuse. Provide layered security and access control.
10	Lifecycle Support	Consider on-boarding to recycling, include decommissioning, and full lifecycle definition for all components that are party to a connected system.
11	Data in Aggregate is Unpredictable	Data stewardship responsibility must be defined. Data may seem innocuous, but can prompt unauthorized usage when in the wrong hands.
12	Plan for the Worst	Disasters can be managed if planned for well ahead – Include capabilities that can help re-issue credentials, reset systems, exclude participants, distribute security patches and updates, and so on, even before they become necessary.
13	The Long Haul	Aging of components, extending lifespan, replacement, wiring in a brownfield environment and evolving of standards and technologies.
14	Attackers Target Weakness	Abide by the principle: 'The strength of the chain depends on its weakest link'. Enforce strong authentication and trust throughout the value chain.
15	Transitive Ownership	Sale and transfer of ownership of components should be possible.
16	N:N Authentication	Each component has multiple roles, actors, user privileges and entitlements; Always consider N:N for complex trust, authentication/authorization schemes.

Juxtaposition of Constrained Environments & Stronger Authentication

A deep dive into RFC 7744 [27] (Use Cases for Authentication and Authorization in Constrained Environments), published by the Internet Engineering Task Force (IETF) can enlighten the security requirements for use cases for varied industries and the same extrapolated to the banking industry.

Golden Rule – Consumer Awareness

Simple human negligence can make artificial or machine intelligence processes vulnerable. An IoT enabled stuffed toy can leak audio/sound prints of a user, and a hacked lightbulb can break Wi-Fi security. Devices, firewalls or governments cannot be held accountable for a data breach, except for the human beings who have designed them for use. Software patches are a reflection of an afterthought stemming from poor security design. Software can be cracked;

networks can be stalked; platforms can be attacked; and users can be tricked. The insecure web of connected things dons no cloak of invisibility and cyber-attacks are imminent when human beings trade security over convenience.

Building security begins at the top and it is everyone's responsibility – be it an IoT device manufacturer, service developer, product configurator or a platform. End consumers need to be aware of the threat of vectors that seem like invisible data; but, a targeted hijacking could be more damaging than a systemic hack. Consumers and enterprises have fast realized the need for trust as a currency, and products/services teams need to build systems of high reputation and brand value.

Bruce Schneier brilliantly summarizes the necessity to build secure systems: "Amateurs hack systems, professionals hack people".

References

- http://www.howtoflyahorse.com/beginning-the-internet-of-things/
- http://spectrum.ieee.org/tech-talk/telecom/security/smartphone-accelerometers-can-be-fooled-by-sound-waves
- OWASP Internet of Things Project https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- "Internet of Things (IoT) Security and Privacy Recommendations", Broadband Internet Technical Advisory Group, Nov 2016. http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
- "IoT Security Guidance", Open Web Application Security Project (OWASP), May 2016. https://www.owasp.org/index.php/IoT_Security_Guidance
- NIST Initiatives in IoT

  https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot
- "Internet of Things Security Companion", Center for Internet Security, Oct 2015

  https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-Controls-IoT-Security-Companion-201501015.pdf
- "Strategic Principles for Securing the Internet of Things (IoT)", US Department of Homeland Security,

Nov 2016. https://www.dhs.gov/securingtheIoT

- GSM Alliance, Feb 2016.

  http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.11-v1.1.pdf

  http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.13-v1.0.pdf

- "Establishing Principles for Internet of Things Security", IoT Security Foundation, undated.

  https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf

- "NYC Guidelines for the Internet of Things", City of New York, undated.

  https://iot.cityofnewyork.us/

- "Principles, Practices and a Prescription for Responsible IoT and Embedded Systems Development", IoTIAP, Nov 2016.

  http://www.iotiap.com/principles-2016_12_02.html

- "IoT Trust Framework", Online Trust Alliance, Jun 2017.

  https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

- "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium, 2016.

  http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

- "Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products", Cloud Security Alliance, 2016.

  https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

- S Gerdes et. al, "RFC 7744: Use Cases for Authentication and Authorization in Constrained Environments", 2016.

  https://tools.ietf.org/html/rfc7744

FROM AN IOT ENDPOINT DEVICE PERSPECTIVE, DEVICES NEED TO POSSESS THE FOLLOWING CHARACTERISTICS: LOW COST AND POWER CONSUMPTION, LONGER LIFE AND PHYSICALLY ACCESSIBLE ENDPOINTS.

Annie Thomas
Product Specialist
TCS Financial Solutions – TCS BaNCS