Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 12, Issue 5

IoT Noir: Instruments of Death

By Wedge Greene

Crime Spree

One Friday on a dark and stormy morning, the young woman entered the clinic procedure room and took the seat that the lab tech directed. She wasn't overtly nervous, but did have a background level of concern. Not so much about her health, but about the inconvenience if an issue was found in her patch micro insulin pump. Not that she expected a problem; yet while the filler cartridges were easy to self-service (she switched hers every Wednesday morning), the bi-annual maintenance was not routine. As the technician logged in the security code and began to read the diagnostic information, she slumped in the chair, dropping her book. The technician looked over, quickly rose to check her pulse and then hit the red emergency button by the door. She was a lucky woman; the pump failure that delivered, all at once, her remaining 5 days of insulin occurred in the clinic.

She received the care necessary to survive.

Friday afternoon, the VP of public relations for the seller of the pump opened an email from a known colleague. Subsequent inspection showed the email address was counterfeit. Within the email was their accident incident report for the young lady. Accompanying this was the diagnostic data from that pump and a log of the commands that had triggered the abnormal release of insulin; it included the internet address of the specific bot that had inserted the attack in the young lady's phone, from there to piggy back on the clinic's system. A polite request for a $100 million 'security consulting fee' to be transferred to an offshore account was balanced by a simple statement that 17% of their customer base was compromised and not delivering insulin; instead, signals were being blocked from the co-deployed monitors of blood sugar levels. Further, the contents of the email would be released to the public, to coincide with bot calls to phones of their compromised customers, if payment was not received by end of banking day.

Post Mortem

Analysis by the manufacturer's team found that the specific event of the pump hack had occurred when the recessed button installed for enabling short term wireless communication from diagnostic center to the device had been pushed by the technician and then accompanied by entry of the manufacturer's decryption key. The manual time-limiting radio enable button had been installed into the pump system design in the pre-release security design audit of their system. It did limit the zone where an outside hack could occur. But the young lady's infected phone was standing by, waiting for this event. This hack required special circumstances. It could be prevented going forward, but there was no assurance that existing devices had not been compromised in prior maintenance cycles.[1]

Finance ran projected loss scenarios based on 'private recall and correction' vs 'exposure of the vulnerability'. They were currently in zero-day stage of vulnerability with only a single threat vector. Release of the bot nets and code at large was the worst case scenario. Calculation of risk (vulnerability vs potential losses) was no longer abstract. Disclosure of security weakness typically removes 10% of a stock's valuation. Recommendation to pay the ransom was made, gaining time for a still costly but manageable private recall. But

they still put in a longshot: calling our (hypothetical) security Private Investigator (PI).

Opportunity Rings

We are now at the beginning of the largest expansion of network and systems; one that follows from the rapid expanse of the Internet but will be orders of magnitude greater and faster. In five years, the number of connected devices is expected to grow from 30 Million to 30 Billion. This is called the Internet of Things [IoT]. It is occurring as more and more devices and systems are enabled with processing control systems, data collection capabilities, and network connection. Outside of hard science fiction, it is difficult to conceive of the transformation this will make in our society. It presents extraordinary opportunities for wonder and productivity. It is also, potentially, the worst thing we can imagine short of the dreaded Singularity. Paraphrasing Jurassic Park's systems scientist Dr. Ian Malcolm, 'first comes the OOHing and AHHing; then comes the running and screaming.'

Connected, interworking product systems of personal, portable blood monitoring and insulin pumps exist today and soon will evolve to become an autonomic pancreas for patients in need. This advance greatly improves the quality of life of its users. It is but one of countless device groups in the future IoT. The infrastructure that supports IoT is just emerging. Inexpensive small processors, cheap Wi-Fi networking chips, sensors, and IPv6 make it possible. Technologies to manage this growth are also emerging, showing a first stage of technology maturity. Deployment of first Fog Computing to manage data streams and later Swarm Computing to allow autonomous local networks will allow reasonable control of the data and network impact.

There is no doubt we are only on the leading edge of the IoT. The growth rate is around 20% per year and still increasing: millions of devices now, 10s of billions in 5 years, 100s of billions in 10 years. Market value estimations only argue about how many trillions of dollars will be generated. Still, the growth of the IoT has a self-limiting factor. It can only increase this fast until every new device we manufacture is connected. While the growth of IoT is exponential now, as new devices are introduced, it will eventually become a logistical curve, its rate of growth reducing when only the already connected device types are replaced. Also, autonomy in devices, as each type gets smarter and more self-reliant, will reduce their need for continuous connection. The development paradigm that 'devices may fail but the system recovers and remains stable' will help contain breaches, localizing them. Unfortunately, the growth of

'first comes the OOHing and AHHing; then comes the running and screaming.'

risk associated with the IoT is not so limited.

Dark Alley

We are moving into a darker world akin to the rise of piracy at the explosive opening growth of maritime commerce. This includes developing threats to the data collected (stolen or altered), threats to the controlling metadata (altered), openings in physical security of devices (hacks), and disruptions in the organization of systems of things (denial of service, failures in communication, failures in infrastructure). In some ways this parallels the first introduction of the firearm as a great force leveler and disruptor of the in-place authority structures. Cyber-sabotage and cyber-espionage attack technologies are proliferating. The threat environment will grow with the following:

- Introduction of new bad guys: organized cybercrime gangs, state sponsored cyber-attacks.
- Introduction of new motives: thievery, ransom, terrorism, industrial espionage, market intelligence, forced technical detent.
- Introduction of new tech: enhanced hacking techniques, new devices with new exploitable openings.
- Continued lack of public will and executive policies that toughen infrastructure.
- Difficulty in developing systems to provide for organization and management of these new IoT networks.

Cisco's estimates of IoT value "discounts future cash flows due to uncertainty around privacy and regulatory issues"[2], aka, security threats are becoming a significant limiter for the corporation's exploitable value from the IoT. Regulatory compliance will add significant costs, skimming IoT potential value, but may help weed out the low-hanging-fruit and starve the marginal hacker.

So how can the security of 100 billion devices be maintained against increasing black hat numbers, better organized operations, and a growing technical sophistication of threat generators? What does our story's security PI do?

Pounding the Pavement

Fortunately, the technology seeds and emerging operational models are present that will allow companies to meet this challenge. But they must be developed, acquired, and deployed rapidly to counter a rapidly increasing threat profile which itself includes growing adaptive capabilities in the bad guys. It has become a race, dollars to be made against dollars to be lost; the economic weather is getting pretty uncertain.

There is a dynamic tension between autonomic systems following ***Self-**** principles of design and the proposed IoT management systems which receive aggregated information streams and push control streams to millions of end node devices. Ironically, the introduction of control software into devices itself becomes a potential opportunity for new attacks. Connected device controls can be usurped; streaming of data from the edge to central clouds can be intercepted. Traditional top-down control models will not suffice. The principle of localization must be used in the development and deployment of global IoT.

Our gumshoe PI in this cyber Noir tale, as with his famous peers, lives in a 'steaming city by the shore'. Commercial system models such as Cisco's Fog computing sit at the shoreline between the sea of devices and the networks and clouds of the interior. This shoreline forms a local management and control interface to a specific offshore 'school' of devices. It filters and aggregates data shipment upstream to cloud analytics. It provides a Policy Management Point for events occurring in the device school. Geoff Brown, CEO Founder of M2Mi, explains another approach to this security landscape:

"Machine to Machine (M2M) interactions in the IoT demand much higher levels of security than previously achieved. M2Mi choose to follow the architecture design of 'highly secure, mission critical infrastructure' often found in the Intelligence Community (IC). Corporate Enterprises and Intelligence Community approaches to security and privacy are vastly different… M2Mi's approach uses powerful security and privacy constructs such as "lockboxes" with whitelists to block all unauthorized communications. Friendly access requires strong verification and validation. This approach hides assets from threats. The security and privacy of Intelligence Community architectures are vastly superior to commercial enterprise approaches in the mission critical infrastructure of IoT ."

He does not abide by all the rules, but he does remain steadfast to his core protective principle. He cares about the young lady with the insulin pump who almost died.

Offshore, the device subnets must also behave like a school of fish. Any individual fish can be eaten, but the school maneuvers to confuse and distract predators – the collective continues. Security systems must develop swarm algorithms that identify an attack and then themselves launch overwhelming counters. These systems embody the altruistic traits of social systems, but the collective behavior of African bee hives swarming on a predator. Security Clouds will be created; ready to react to notifications from analytic clouds which identify the existence and source of an attack. These counter-attack clouds will launch blocking swarm agents on the attacker. I expect that even botnets will be used as friendly security antibodies. Built into devices and systems as they are distributed, they wait for an Operations command to launch counter strikes against security attacks.

Confronting the Guilty

Our gumshoe PI is not a pretty guy. He does not abide by all the rules, but he does remain steadfast to his core protective principle. He cares about the young lady with the insulin pump who almost died. Sweat is needed to find the bad guy. Violence is a tool to be used to curb violence. Yet he lives in a world where authority and order also exist; he packages his findings and provides it to the courts for dispensing justice.

Unfortunately, his bureau of cyber enforcement and court of justice does not currently exist in our world. There is no agency that effectively enforces international law on cybercrime. Bilateral cyber treaties have no teeth. These laws and systems need development. This means growing the collaborative consortia where standard's business gets done today. The ITU has dozens of security standards and guidelines. The web consortia have the Open Web Application Security Project (OWASP). So also security groups exist in the TeleManagement Forum (TMForum) and the Industrial

Internet Consortium (IIC). This is a start: security frameworks are scrubbed out but not fleshed out (aka Industrial Internet Reference Architecture.) Test-beds are being proposed and some are being enabled. Alan Sill of the NSF center for Cloud and Autonomic Computing (CAC) is recommending the academic and standards community implement CloudLab for very-large research tests. Yet each of these approaches is a specialist in a finite organization.

So no sharp international court room thrillers are expected in our eReader inbox. Returning to our prediction, these times are getting darker. Storm Clouds are developing. Our Noir cyber tale is still about a gumshoe pounding dirty alleys and this is just the beginning.

---

[1] This fictional scenario was adapted from [A Review of the Security of Insulin Pump Infusion Systems; J Diabetes Sci Technol. 2011 Nov; 5(6): 1557–1562. Published online 2011 Nov 1] and [Insulin Pumps Vulnerable to Hacking; Published August 04, 2011; Associated Press].

[2] The Internet of Everything (IoE) Value Index. Cisco web site.