Machina
Research

Securing the Internet of Things - an Analyst's View of the Market

December 2016, IoT Security Foundation

Aapo Markkanen, Principal Analyst
@markkaapo

About Machina Research

- **Machina Research is the world's leading provider of market intelligence and strategic insight on the rapidly emerging Internet of Things, Machine-to-Machine (M2M) and Big Data opportunities.**

- **We provide market intelligence and strategic insight to help our clients maximise opportunities from these rapidly emerging markets. If your company is a mobile network operator, device vendor, infrastructure vendor, service provider or potential end user in the IoT, M2M or Big Data space, we can help.**

- **We work in two ways:**
    - Our **Advisory Service** consists of a set of Research Streams covering all aspects of IoT and M2M. Subscriptions to these multi-client services comprise Reports, Research Notes, Forecasts, Strategy Briefings and Analyst Enquiry.
    - Our **Custom Research and Consulting** team is available to meet your specific research requirements. This might include business case analysis, go-to-market strategies, sales support or marketing/white papers.

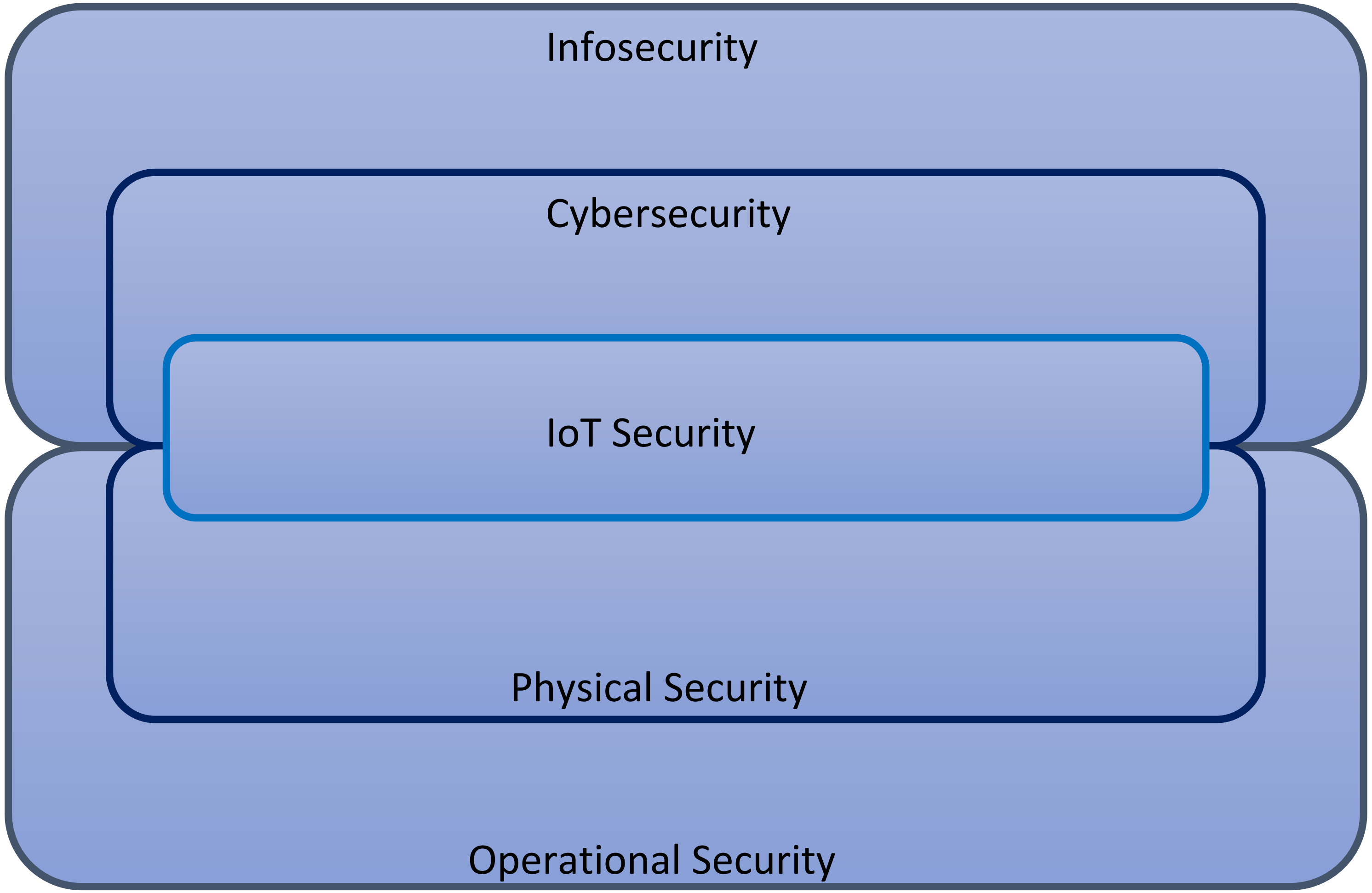
- **The company was founded in 2011 by Matt Hatton and Jim Morrish, two experienced industry analysts and the team has grown substantially since then.**

- **Acquired by Gartner in November 2016.**

Session agenda

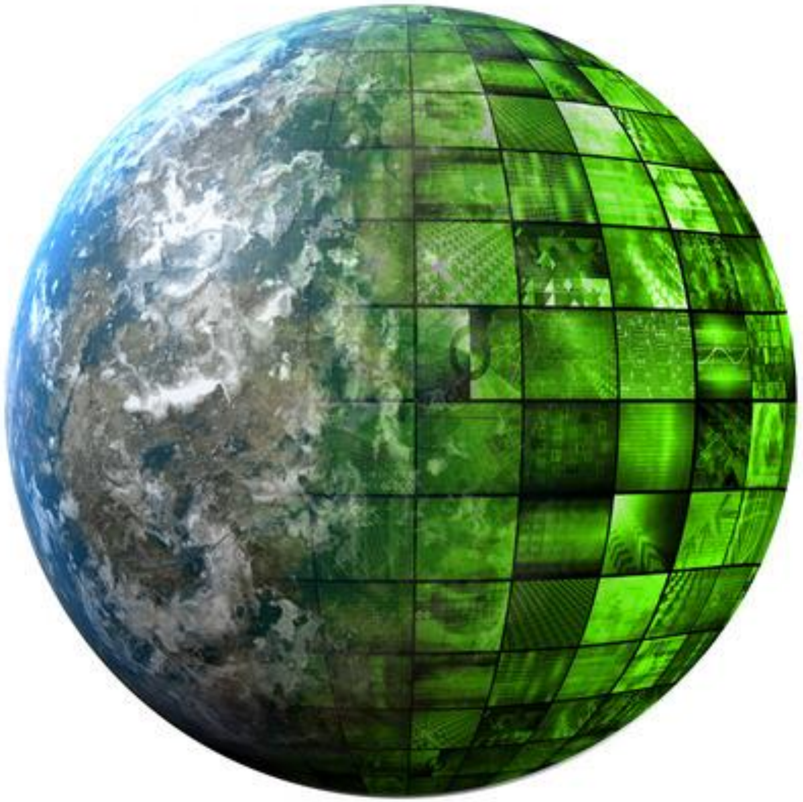
- Setting the scene
- Strategic guidelines
- Building blocks
- Concluding remarks

What is IoT security, anyway?



What makes it different (and difficult)

- **Physical consequences of incidents**
  - Things can blow up
- **Geographically dispersed endpoints**
  - Can't just build that (fire)wall
- **Constrained operating environments**
  - Tricky form factors and battery power make life complicated
- **Complex supply chains**
  - You may be secure, but are all your sub-sub-subcontractors?
- **Extensive legacy issues**
  - Brownfield's way tougher than greenfield
- **Untested business models**
  - Security has to support the business case…if you have one
- **Nascent regulatory regimes**
  - Whose fault is it if Things do blow up?



Four thrusts towards a secure IoT

- Security by risk management
- Security by application assessment
- Security by design
- Security by systems integration

Security by risk management

- **Security is never a binary choice of either having it or not having it**
  - The security layer can be enabled by a huge variety of product/service combinations

- **It is possible to have “too little” as well as “too much” of security**
  - Security shouldn’t jeopardise the business case or the user experience

- **“What is the worst that can happen? And how probable is it to happen?”**
  - Judge carefully how much risk you can handle – and invest accordingly

Security by application assessment

- **Application diversity makes "IoT security" almost an oxymoron**
  - A light bulb and an industrial control system are not the same

- **There are differences (and further divergence) between geographies**
  - Especially privacy regulations are a big factor – see the EU and GDPR

- **Use cases add further context – and can be hard to predict**
  - Having a voice-controlled TV is riskier in a board room than in a living room

Security by design

- **Security should never be an afterthought**
  - …unless it has to be

- **Smart products are difficult to secure. Smart systems are even more so**
  - Consumer IoT tends to be greenfield. Enterprise IoT tends to be brownfield

- **Gateways to the rescue**
  - “Intelligent” IoT gateways can secure brownfield and future-proof greenfield

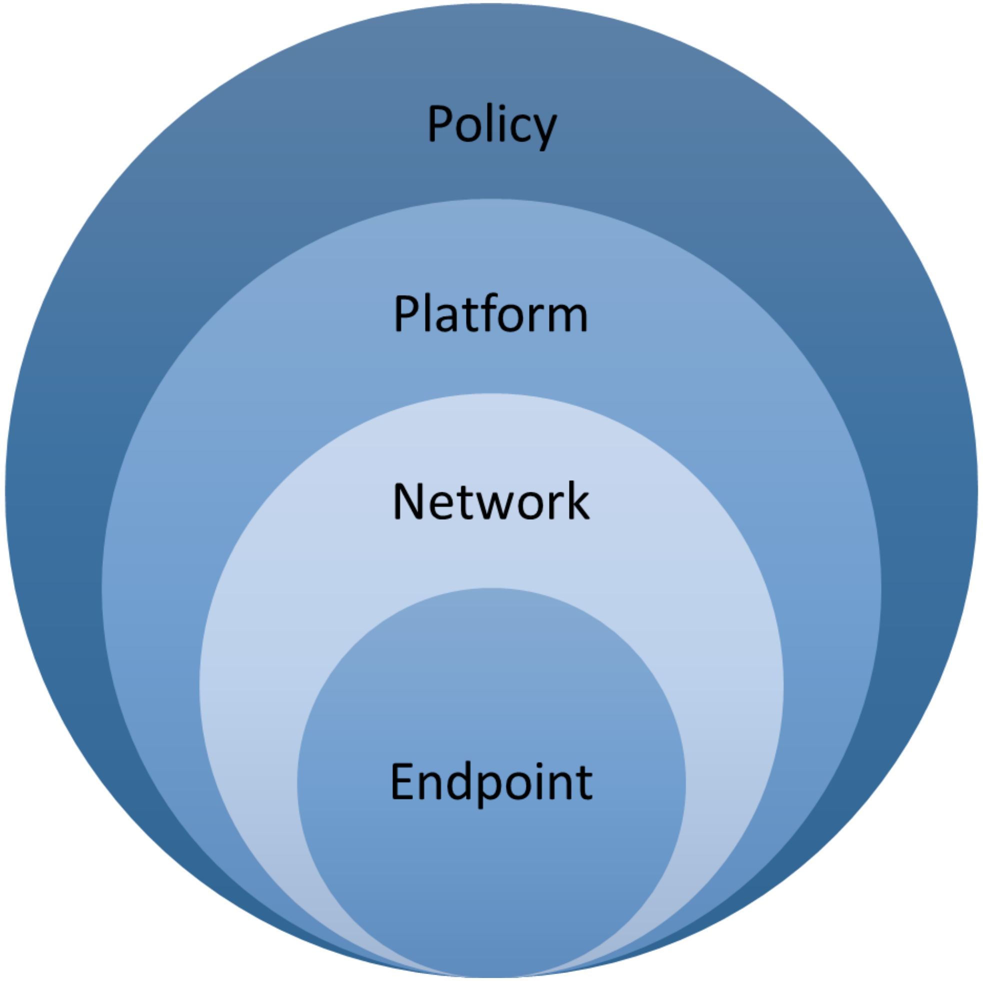
Security by systems integration

- **Smart systems = different products from different suppliers at different times**
  - Deployment complexity means that security gaps are more or less inevitable

- **To minimise the gaps, someone has to take special ownership of security**
  - The SI or the lead OEM is the most natural “owner” for the security layer

- **SIs will become the single most critical stakeholder in IoT security**
  - …so too bad they aren’t too good at it. At least yet

Security layer layered



Policy

Platform

Network

Endpoint

Key technology elements

- **Root of Trust**
  - Hardware-based trust more robust than software-based
  - Lots of innovation on the silicon level – but lots of fragmentation too

- **Cryptography**
  - PKI isn't going away, but it has to evolve under the IoT
  - Sea change from RSA to ECC?

- **Threat intelligence and analytics**
  - By far the hottest area in today's cybersecurity
  - Lots of promise in securing complex (but stable) IoT systems, in particular

- **Device management**
  - Becoming increasingly table stakes in IoT security
  - Convergence of Enterprise IoT and Enterprise Mobility?

Coming up in technology (a bit later)

- **Virtualisation and hypervisors**
  - Growing demand for more sophisticated isolation techniques
  - Spreading beyond the traditional (i.e. hell expensive) embedded systems

- **Fog computing**
  - Gateways will be important – the fog paradigm will take them to the next level
  - More advances in SDN/NFV needed to make the fog a reality

- **Blockchain and distributed ledger**
  - “Pure” blockchain may be fantasy in the IoT, but the distributed ledger as such is not
  - Again, something for complex systems, especially in Subnets of Things

- **Quantum computing**
  - May well mess up everything within 10-15 years – or may not
  - In theory, any new critical infra should already be deployed as quantum-safe

Of course, it’s not only about tech

- Using a state-of-the-art technology does no good if the process and policy are substandard
- The recent DDoS frenzy is a process problem, rather than a technology problem
- Guidelines, frameworks, and best practices can improve the situation – but only up to a point
- Getting the process side right requires the right kind of people and, thus, money
- Ultimately, manufacturers and developers need to have enough incentive to take security seriously
- If the incentive simply is not there, we need more/better regulation to change the dynamic

Concluding remarks

- IoT security is as diverse as the IoT itself. So let's be careful with generalisations
- Products and systems are very different. Products are secured by design, systems by integration
- Security for Enterprise IoT is relatively advanced. Security for Consumer IoT is anything but
- Much of today's innovation involves gateways. They will be instrumental also in the long term
- Security analytics is showing a lot of promise. Safe to expect AI to be huge for IoT security
- All security issues don't need to be addressed right now. So don't let them hold you back too much
- In many cases, security problems aren't about tech – but process, policy, and (especially) incentive

Thank you!

Aapo Markkanen
Principal Analyst,
Machina Research

@markkaapo
aapo.markkanen@machinaresearch.com