

Жизнь без хлопот в мире IoT

Денис Кравченко

Специалист отдела информационной безопасности,
"Vodafone Ukraine"

Denys Kravchenko

IT Security Specialist,
"Vodafone Ukraine"

E-mail: kravchenko.denys@gmail.com
dekravchenko@vodafone.ua



Предистория вопроса

- **Встраиваемая система** (встроенная система, англ. embedded system) — специализированная микропроцессорная система управления, концепция разработки которой заключается в том, что такая система будет работать, будучи встроенной непосредственно в устройство, которым она управляет.
- Распространенность;
- Доступность;
- Ограниченная функциональность;
- Относительная беззащитность;
- Работоспособность важнее безопасности;
- Превалирование проводных технологий доступа;
- Устаревшая модель угроз;

Предистория вопроса

- **Machine-to-Machine, M2M** — общее название технологий, которые позволяют машинам обмениваться информацией друг с другом, или же передавать её в одностороннем порядке. Это могут быть проводные и беспроводные системы мониторинга датчиков или каких-либо параметров устройств (температура, уровень запасов, местоположение и т. д.).
- В Европе крупнейшими операторами является Telefonica в Испании, Telenor (Скандинавия), Orange Business Services (входит в France Telecom) и Vodafone.
- По оценкам МСЭ 50 млрд. устройств будут подключены к интернету к 2020 году.

Настоящее время

- **Интернет вещей (англ. Internet of Things, IoT)** — концепция вычислительной сети физических объектов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой[1], рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.
- Облачные вычисления;
- Программно-определяемые сети;
- IPv6;
- Новые стандарты и протоколы связи - 5G;
- Успехи в разработке миниатюрных и долговечных источников питания;

Различия между M2M и IoT

M2M

- Connected devices and associated applications
- Fixed solution parameters
- Rigid solution architecture
- 'Speed' designed in where necessary
- Applications in the context of verticals and niches
- Data is meaningful in context
- Structured data
- Predictable growth (in connections and data generated)
- Data ownership often clear



IoT

- Complex applications and data analysis
- Heterogeneity and flexibility of solution components
- Distributed and federated processing, storage and querying
- 'Speed' needs to be supported as and when requirements emerge
- Data disassociated from any source
- Semantic richness, shared context and ontologies
- Semi-structured and unstructured data
- Unpredictable growth driven by network effects
- Data ownership often very unclear

Некоторые международные институты участвующие в стандартизации IoT

- ISO;
- МСЭ (группа ITU-IT SG20);
- GSMA;
- GlobalPlatform;
- IoT Forum-ы;
- Альянсы (LoRa Alliance, другие);
- Open Source сообщества (OASIS — MTT Message Queuing Telemetry Transport);
- Другие заинтересованные стороны (oneM2M, OMA, ...);

У каждого свое видение, пожелания, особенности, ...

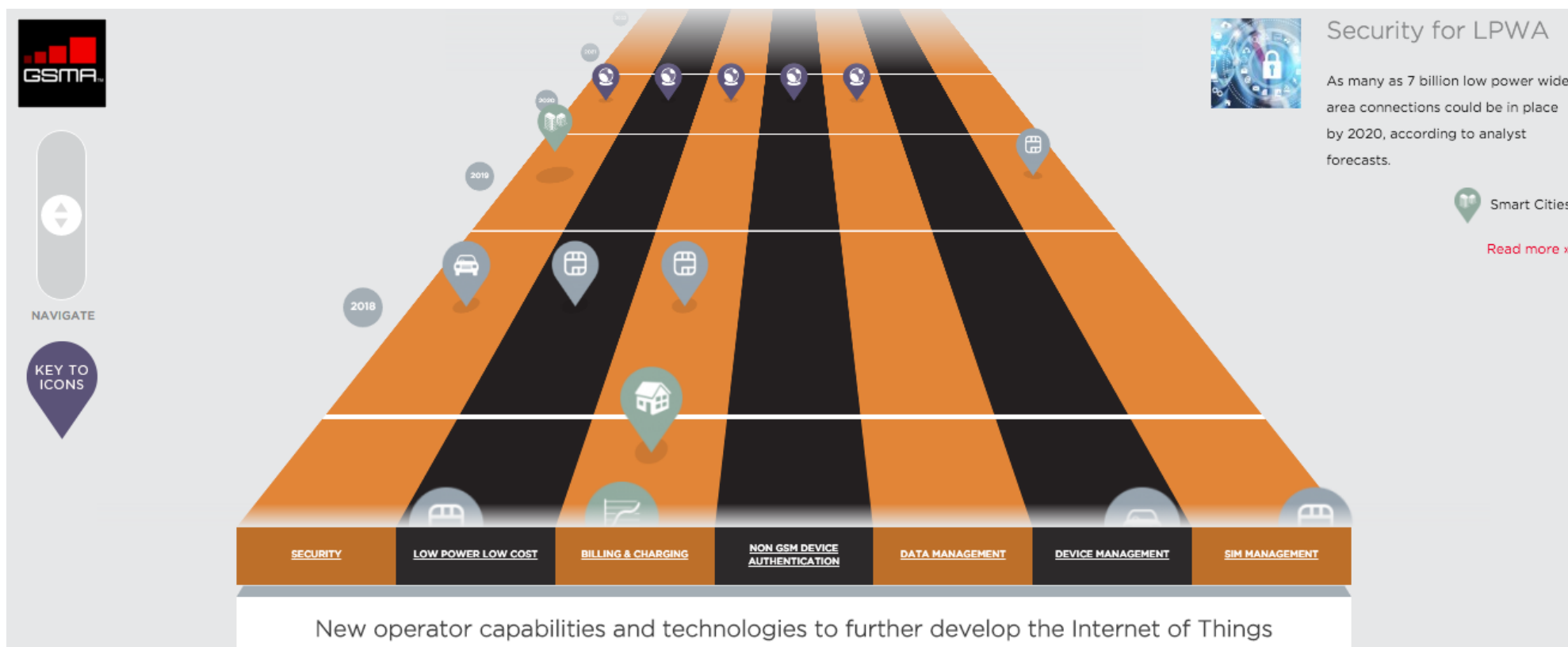
Направления стандартизации

- Архитектура;
- Интерфейсы взаимодействия;
- Протоколы;

Общие требования к IoT

- Универсальность;
- Дешевизна;
- Массовость;
- Вандалоустойчивость;
- Легкость в администрировании;
- Небольшая нагрузка на канал связи;
- Работа в условиях постоянной потери связи или других проблем на линии, «сеансовость» связи;
- Отсутствие ограничений на формат передаваемого контента;
- Низкая потребляемая мощность;
- Безопасность;

Примеры - <http://gsma-future-iot-networks.com>



Примеры — onem2m.org

onem2m.org/technical/published-documents

РАН SHARING SIP Выполнен импорт Блокнот Выполнен импорт (1) Импортировано из Mobicents conference.hitb.org/ Newplow. Soft

и страницы английский Хотите перевести ее? Нет Перевести Всегда переводить английский Парам

oneM2M Standards for M2M and the Internet of Things [Member Login](#)

HOME ABOUT ONEM2M ▾ MEMBERSHIP ▾ INSIGHTS ▾ **TECHNICAL ▾** NEWS & EVENTS ▾ Search...

You are here: [Home](#) > [Technical](#) > [Published Specifications](#)

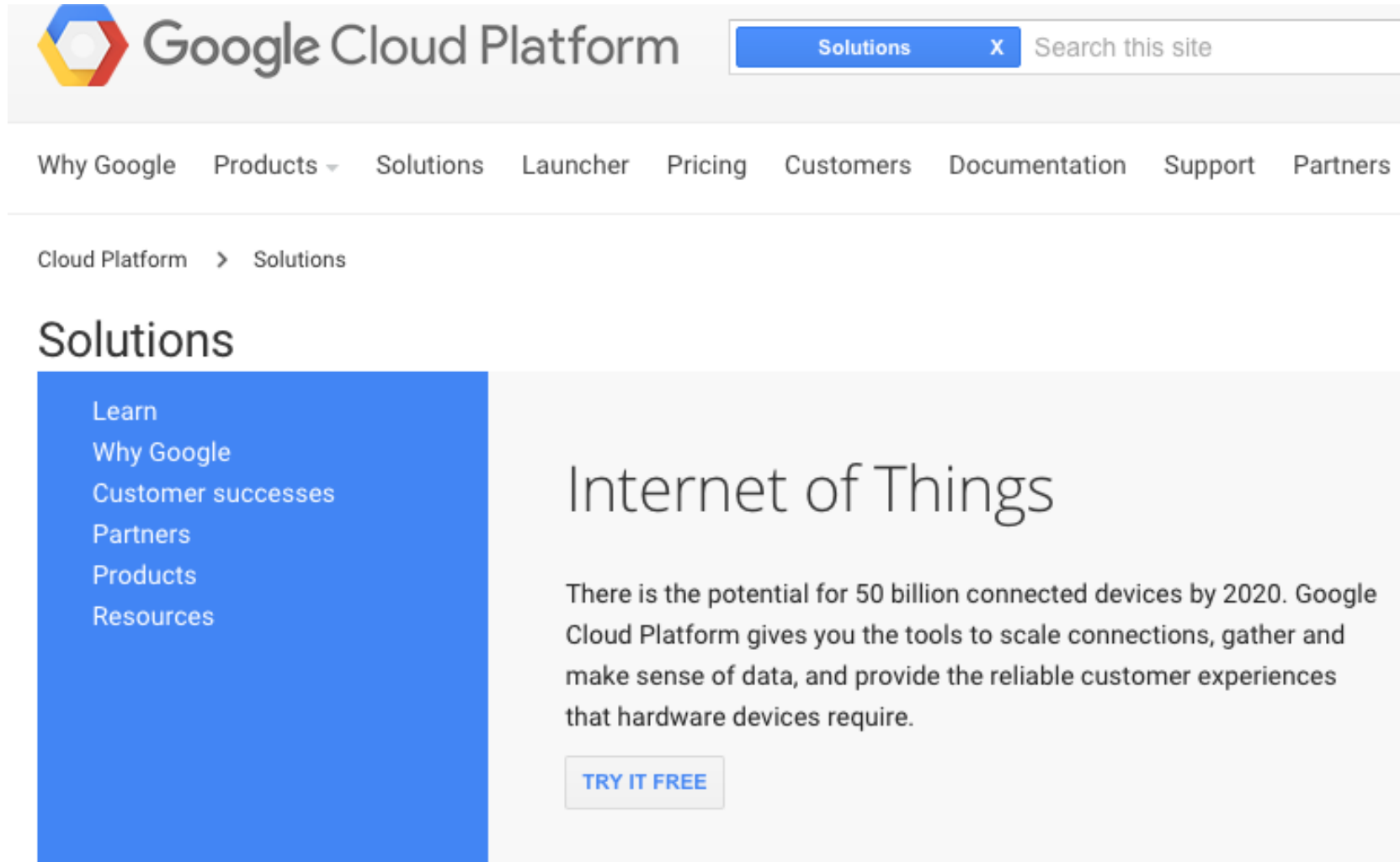
Published Specifications

As we publish new specifications, they will appear here or on release-specific pages. [Print](#) [Email](#)

oneM2M Release 1 specifications

Reference	Version	Title	Date	ARIB	ATIS	CCSA	ETSI	TIA	TTA	TTC
TS 0001	1.6.1	Functional Architecture	01/2015		ATIS.oneM2M.TS0001V161-2015		TS 118 101 V1.0.0		TTAT.MM-TS.0001	TS-M2M-0001v1.6.1
TS 0002	1.0.1	Requirements	01/2015		ATIS.oneM2M.TS0002V101-2015		TS 118 102 V1.0.0		TTAT.MM-TS.0002	TS-M2M-0002v1.0.1
TS 0003	1.0.1	Security Solutions	01/2015		ATIS.oneM2M.TS0003V101-2015		TS 118 103 V1.0.0		TTAT.MM-TS.0003	TS-M2M-0003v1.0.1
TS 0004	1.0.1	Service Layer Core Protocol Specification	01/2015		ATIS.oneM2M.TS0004V101-2015		TS 118 104 V1.0.0		TTAT.MM-TS.0004	TS-M2M-0004v1.0.1
TS 0005	1.0.1	Management Enablement (OMA)	01/2015		ATIS.oneM2M.TS0005V101-2015		TS 118 105 V1.0.0		TTAT.MM-TS.0005	TS-M2M-0005v1.0.1

Поддержка



The screenshot shows the Google Cloud Platform website's 'Solutions' section. At the top, the Google Cloud Platform logo is on the left, and a search bar with 'Solutions' and a close button 'X' is on the right. Below the logo, a navigation menu includes 'Why Google', 'Products', 'Solutions', 'Launcher', 'Pricing', 'Customers', 'Documentation', 'Support', and 'Partners'. A breadcrumb trail shows 'Cloud Platform' followed by a right arrow and 'Solutions'. The main heading 'Solutions' is on the left. A blue sidebar contains links: 'Learn', 'Why Google', 'Customer successes', 'Partners', 'Products', and 'Resources'. The main content area features the heading 'Internet of Things', a paragraph about the potential for 50 billion connected devices by 2020, and a 'TRY IT FREE' button.

Google Cloud Platform

Solutions X Search this site

Why Google Products Solutions Launcher Pricing Customers Documentation Support Partners

Cloud Platform > Solutions

Solutions

- Learn
- Why Google
- Customer successes
- Partners
- Products
- Resources

Internet of Things

There is the potential for 50 billion connected devices by 2020. Google Cloud Platform gives you the tools to scale connections, gather and make sense of data, and provide the reliable customer experiences that hardware devices require.

[TRY IT FREE](#)

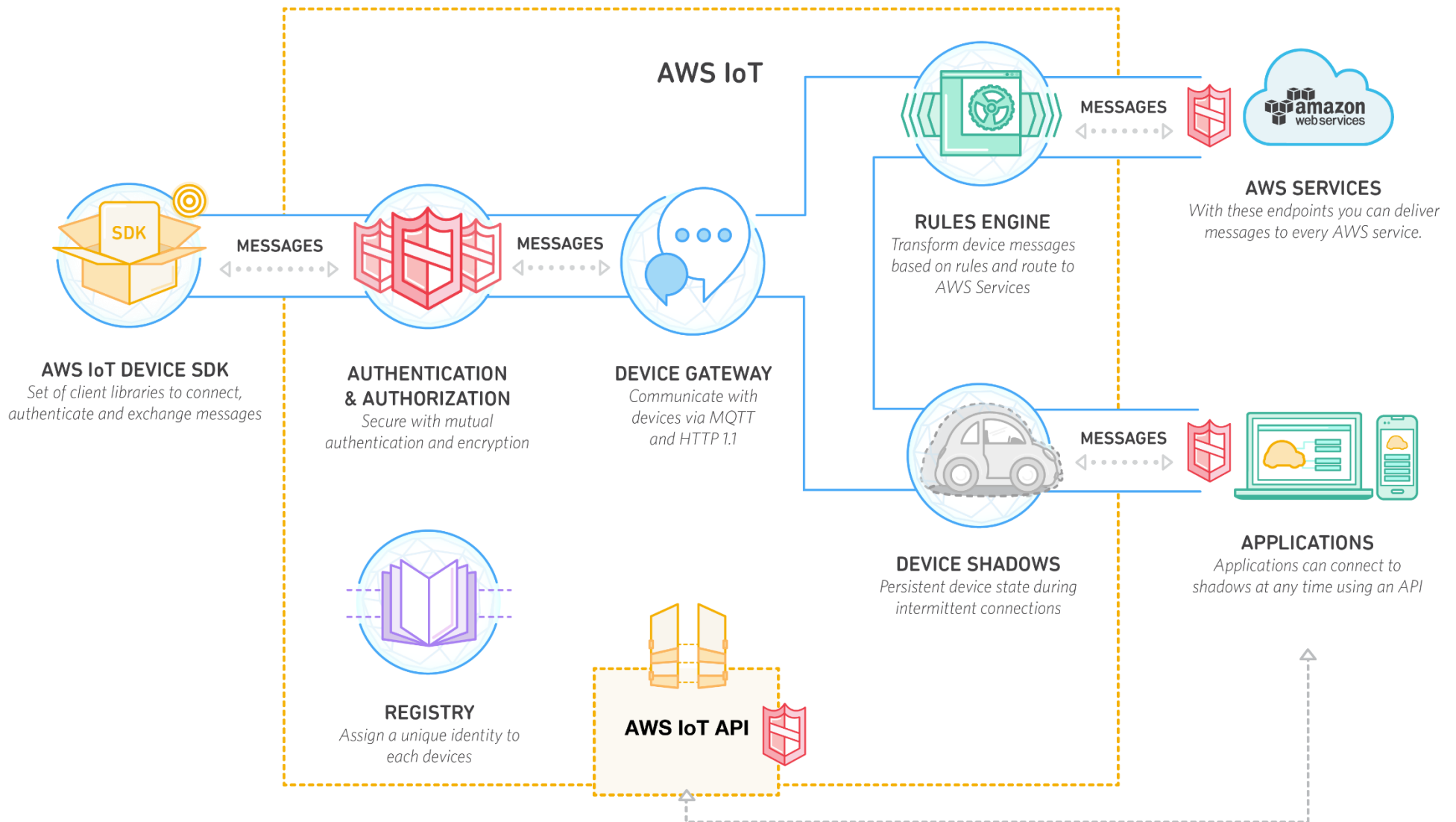
Поддержка



Credit: Thinkstock

Azure IoT Suite attracts with plenty of device SDKs including C#, but some pieces are still missing

Поддержка



Типовые механизмы обеспечения безопасности конечных устройств IoT



ARTIK™

HARDWARE SECURITY

- Unique ID Certificate
- Chip Manufacturer and OEM Cryptographic Keys
- Common Criteria EAL 5+ Certification

REMEDiation SUPPORT

- Secure Firmware Updates



PLATFORM SECURITY

- Secure Boot
- Runtime Integrity
- Key Based Authentication
- Trusted Execution Environment (TEE)
- Storage Encryption
- TLS/DTLS Network Data Encryption
- Local Intelligence
- Anomaly Detection
- Secure pairing/Geo-Fencing
- Data Replication and Device Failover

Некоторые протоколы взаимодействия и передачи информации

Protocol	CoAP	XMPP	RESTfulHTTP	MQTT
Transport	UDP	TCP	TCP	TCP
Messaging	Request/ Response	Publish/ Subscribe Request/ Response	Request/ Response	Publish/ Subscribe Request/ Response
2G, 3G, 4G Suitability (1000s nodes)	Excellent	Excellent	Excellent	Excellent
LLN Suitability (1000s nodes)	Excellent	Fair	Fair	Fair
Compute Resources	10Ks RAM/ Flash	10Ks RAM/ Flash	10Ks RAM/ Flash	10Ks RAM/ Flash
Success Stories	Utility Field Area Networks	Remote management of consumer white goods	Smart Energy Profile 2 (premise energy management, home services)	Extending enterprise messaging into IoT applications

Стандарты безопасности для IoT (дополнительно)

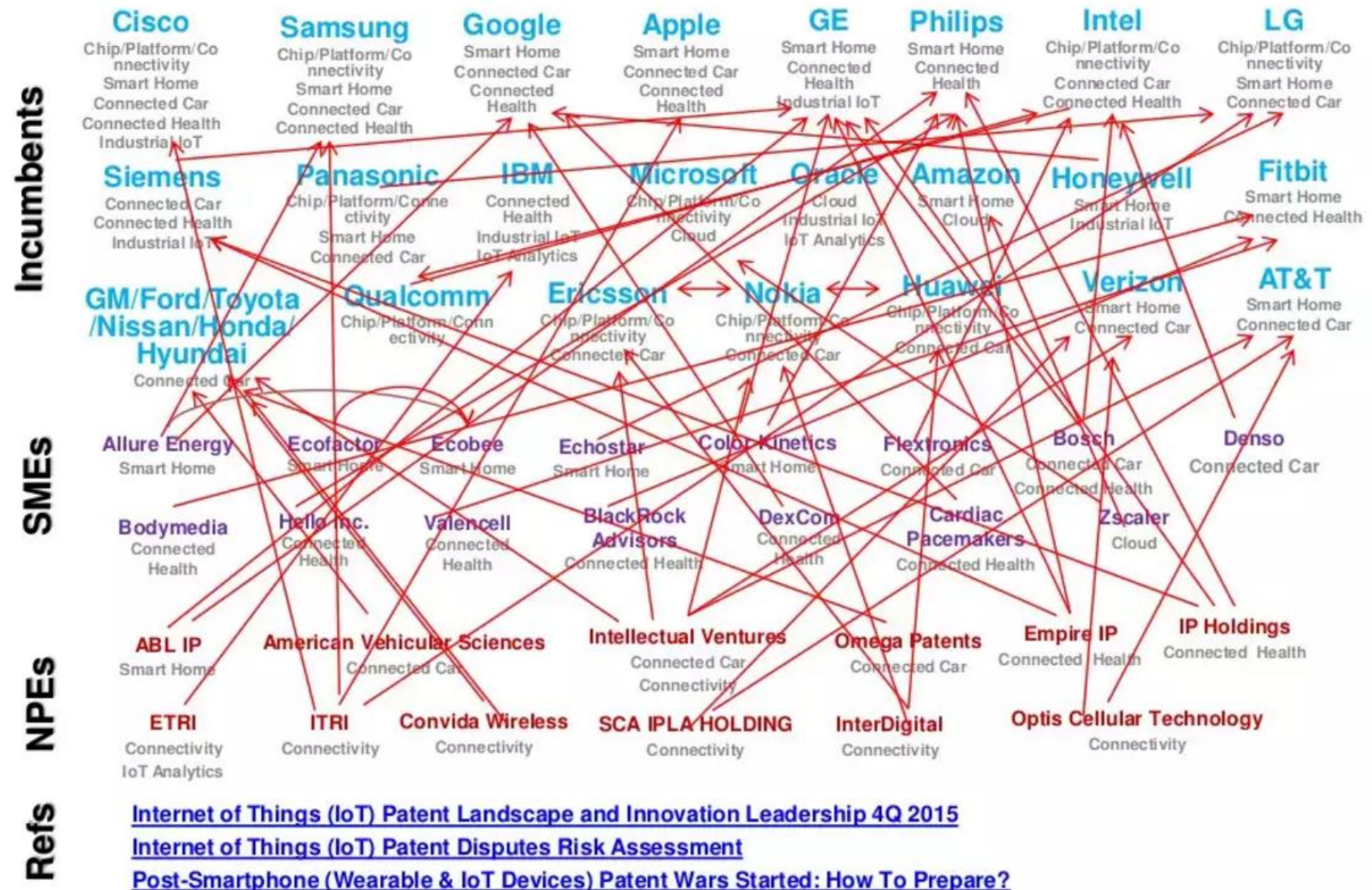
- Common Criteria;
- FIPS (FIPS 140-2);
- Java-card;
- PCI DSS;
- Embedded System Security Best Practices;
- Отраслевые стандарты космонавтики, авиации, стандарты безопасности для систем реального времени и поддержки жизнеобеспечения;
- Ассоциации производителей автомобилей (Self-driving cars Safety);

Типовые проблемы общей стандартизации

- «Свои» решения в качестве стандартов;
- Отраслевая замкнутость;
- Дискриминационные альянсы;
- Высокие патентные отчисления и роялти;
- Стандартизация существующих (не лучших) решений для ускорения времени окупаемости и уменьшения времени выхода на рынок;

Типовые проблемы общей стандартизации - патенты

Internet of things (IoT) Patent Wars 2020 Scenarios Infographics



Причины проблем безопасности IoT

- Ограниченный объем источника питания;
- Малая вычислительная мощность;
- Часто отсутствие реализации механизмов безопасных вычислений (SE, TEE, ...);
- Невозможность реализовать механизмы безопасности из-за требуемой низкой стоимости;
- Возможность атак по отводным каналам side-channel attack и ПЭМИН;
- Локальные требования законодательства в глобализированном мире (роуминг для M2M);
- Затруднен контроль безопасности - несколько участников схемы IoT;

Прогнозы по проблемам безопасности M2M/IoT

- Zombified Internet of Things (IoT);
- Невозможность исправить появившиеся проблемы в кратчайшие сроки (отсутствует возможность обновлений, удаленного доступа, ...);
- Формирование недостоверных отчетов и прогнозов из-за массово взломанных/модифицированных датчиков, и, как следствие, принятие неправильных решений, могущих привести к техногенным катастрофам;
- Тотальный контроль/шпионаж (снижение уровня демократичности отдельных стран);
- Установление контроля более высокотехнологичных стран над менее технологически развитыми странами;
- Уменьшение возможностей по борьбе с терроризмом;
- Компрометация персональных данных и конфиденциальной информации;

Примеры проблем по безопасности M2M/IoT



**The Internet of Things That Talk
About You Behind Your Back**



Written by
BRUCE SCHNEIER

IoT Next Surveillance Frontier, Says US Spy Chief US Director of National Intelligence James Clapper delivers chilling remarks regarding the Internet of Things, noting there may come a day when spy agencies may tap into IoT for surveillance, network access, and more.

09.02.2016, James Clapper told US Senate members - "In the future, intelligence services might use the [Internet of Things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials".



НОВЫЕ ВОЗМОЖНОСТИ

- Медицинские датчики;
- Производственные датчики;
- Кастомизация через детальную персонификацию;
- Высоко-целевая реклама (при ее деперсонализации);



Уровень стандартизации безопасности IoT и его важность

- Безопасность IoT вынесена на уровень национальной безопасности в США:

To address the security of IoT devices, President Obama's new **Cybersecurity National Action Plan**, introduced 09.02.2016, calls for establishing a testing and certification center for IoT devices:

The Department of Homeland Security is collaborating with UL and other industry partners to develop a Cybersecurity Assurance Program to test and certify networked devices within the “Internet of Things,” whether they be refrigerators or medical infusion pumps, so that when you buy a new product, you can be sure that it has been certified to meet security standards.

(<https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>)

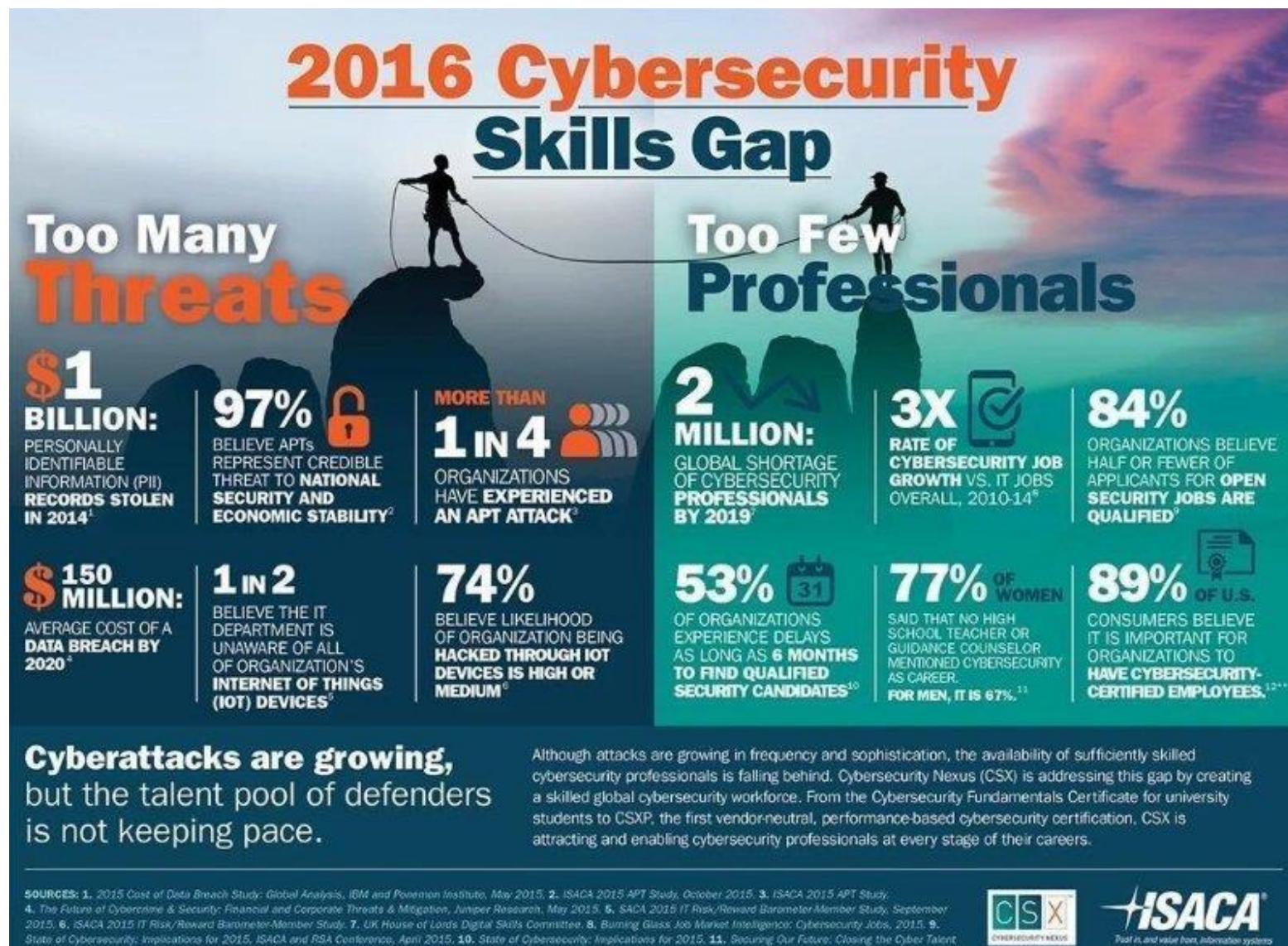
Украина — РНБО утвердила новую стратегию кибербезопасности страны.



Адаптация - метод замены обложки (потенциальные проблемы) или изобретение велосипеда



Стандартизация безопасности IoT—кадры решают все :-)



Заключение:

- Необходимо выполнить большой объем работ по унификации существующих стандартов IoT;
- Выработать общие принципы и подходы к обеспечению безопасности IoT, с применением основных принципов (минимальная достаточность, ...).
- Адаптировать национальные законодательства и стандарты с учетом лучших мировых практик и международных стандартов.

Использованные материалы:

1. www.ISO.org
2. www.GSMA.com
3. www.ETSI.org
4. www.onem2m.org
5. www.Microsoft.com
6. www.Amazon.com
7. <http://blogs.cisco.com/ioe/beyond-mqtt-a-cisco-view-on-iot-protocols>
8. http://motherboard.vice.com/en_ca/read/the-internet-of-things-that-talk-about-you-behind-your-back
9. www.techipm.com



Спасибо за внимание!

Контакты:

Денис Кравченко
Denys Kravchenko

E-mail:

kravchenko.denys@gmail.com
denys@outlook.com
dekravhenko@vodafone.ua

Mobile:

+380504102957
+380994197999

Skype: denys.kravchenko

Социальные сети:

Facebook	-	https://www.facebook.com/kravchenko.denys
Twitter	-	@DenysKravchenko
Linkedin	-	https://ua.linkedin.com/in/denys-kravchenko-492a4515

