



A World of Connected Objects Designed to Serve Us

Philip Andreae

Philip@Andreae.com

10 October 2017

Identity

Authentication

Identification

Authorization

Four Words

Independent and Inseparable

Privacy

Security

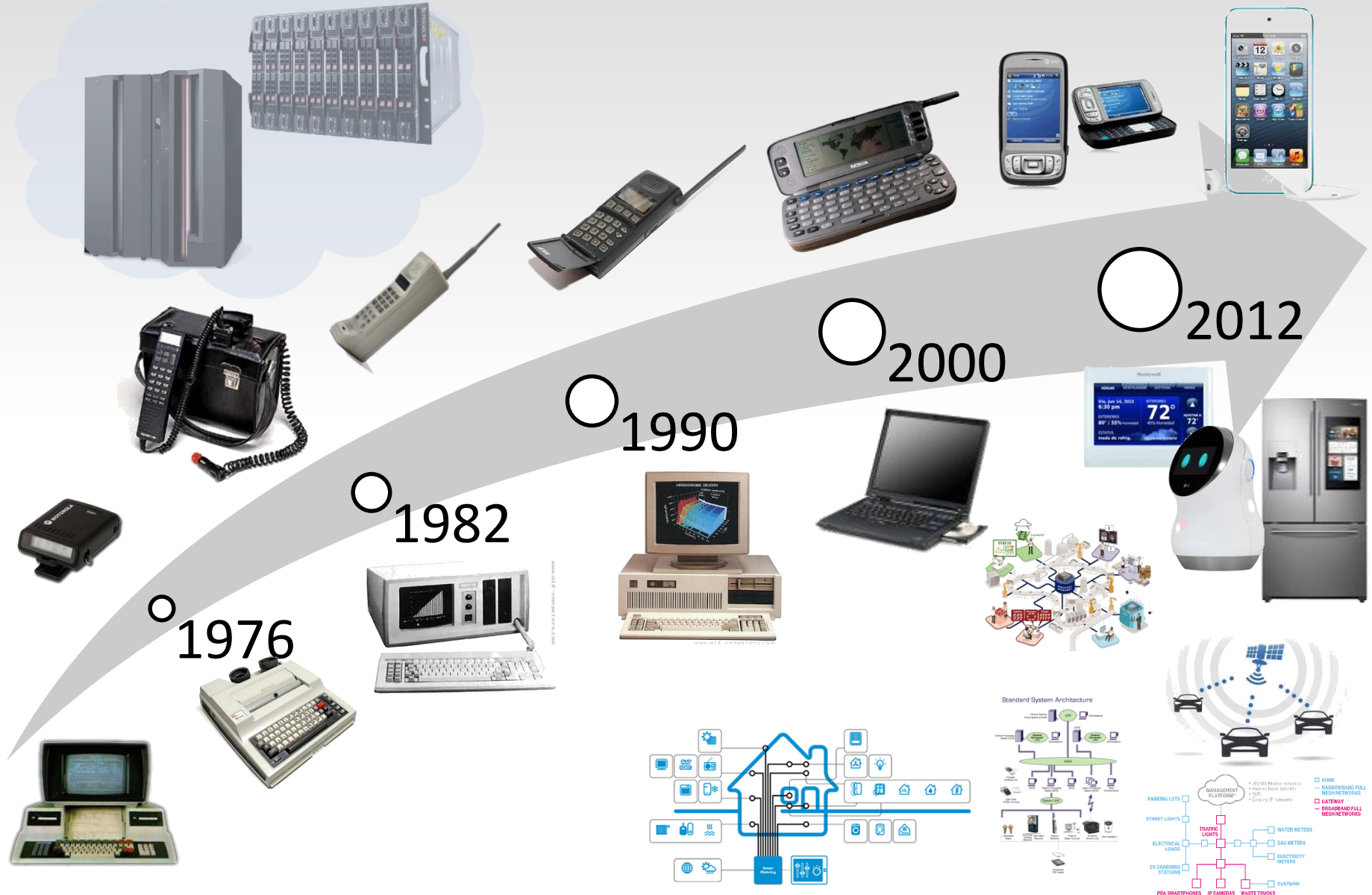
Confidentiality

Three Concerns

Lost as we engage and leave tracks

We Live in a Age of Connected Things

pa



With A Need To Enhanced Digital Security To Protect Our Daily Life

pa

EUROPAY
International



VISA

In 1993 six people from three payment schemes met at Hotel at O'Hare airport and agreed to work together to define a common set of requirements and subsequently published ***"The Integrated Circuit Card Specifications for Payment Systems"***

The goal Global Interoperability allowing each region and nation to decide when to migrate from Magnetic Stripe to the EMV Standard

EMVCo is owned & staffed by Visa, MasterCard, JCB, American Express, UnionPay and Discover

Counterfeit Protection

Off/On-line Authentication

Offline Authorization

Cost Reduction



Lost and Stolen Fraud

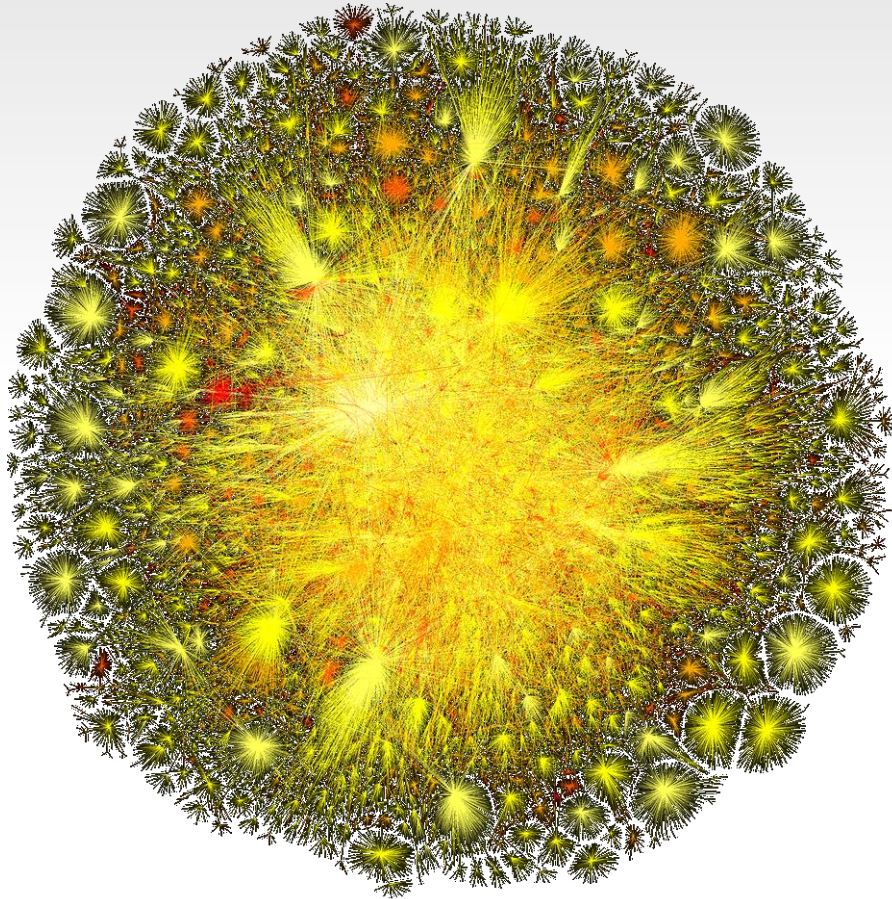
Cardholder Verification

Revenue Creation

Value Added Services

Digital Identity in a Digital World is a Challenge

pa



The Internet at the MOMA



The New Yorker

- FIDO is the World's Largest Ecosystem for Standards-Based, Interoperable Authentication
 - Better security for online services
 - Reduced cost for the enterprise
 - Simpler and safer for consumers
 - Deploy Your Online Authentication Using Open and Scalable Standards
- The specifications and certifications from the FIDO Alliance enable an interoperable ecosystem of hardware-, mobile- and biometrics-based authenticators that can be used with many apps and websites.
- This ecosystem enables enterprises and service providers to deploy strong authentication solutions that reduce reliance on passwords and protect against phishing, man-in-the-middle and replay attacks using stolen passwords.
- The mission of the FIDO Alliance is to change the nature of online authentication by:
 - Developing technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users.
 - Operating industry programs to help ensure successful worldwide adoption of the Specifications.
 - Submitting mature technical Specification(s) to recognized standards development organization(s) for formal standardization.



Multi-Factor Authentication

- Something You Have ✓ The Token = Card/**Phone**
- Something You Know ✓ The Secret = PIN/**Password**
- Something You Are ✓ Biometric = You

EMV, PIV, ICAO, eID, FIDO ... Exploit

- ✓ The security of hardware
- ✓ The flexibility of software
- ✓ The power of cryptography

Measure
Meter
Collect
Control
Stimulate
Manipulate
Support
Pay
**Connected
Commerce**

Integrate into our Homes
Manage City Infrastructure
Enhance Healthcare
Automate Factories
Control Automobiles
**Enhance the
Consumer Experience**

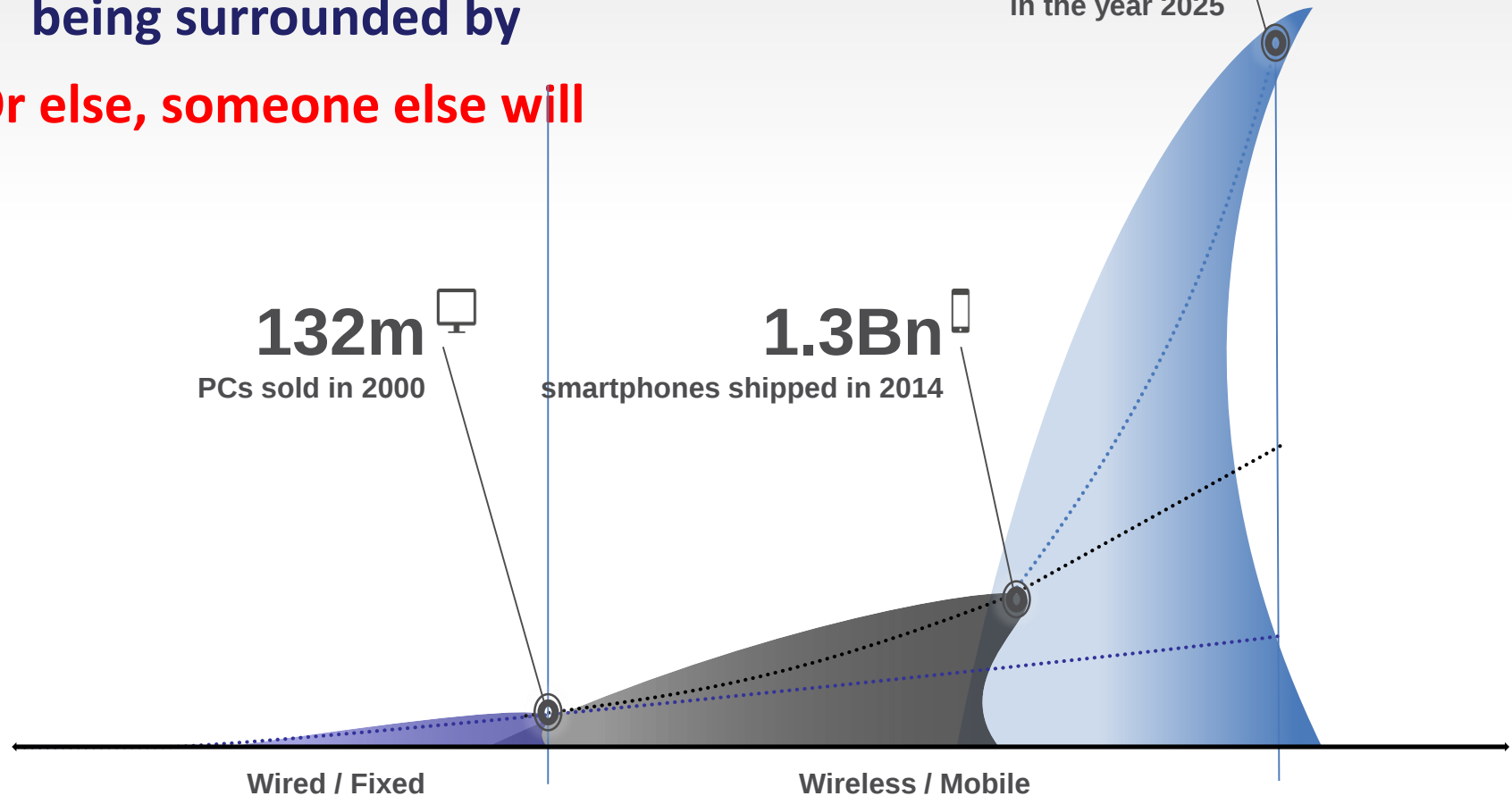
The World of Objects and Things is Exploding

pa

We must
Identify and Authenticate
these objects we are
being surrounded by
Or else, someone else will

10s of Billions

Of connected objects will exist
in the year 2025



National Defense, Criminals & State Actors and Terrorists

- Denial of Service
- Phishing
- Vishing
- Hacking
- Counterfeiting
- Stealing
- Terrorizing

- Google
- Sony
- Target
- Office of Personal Management
- Equifax
- Democratic National Committee
- And so many more

Wikipedia lists 244

A limited publicly acquired sample

https://en.wikipedia.org/wiki/List_of_data_breaches

To amplify the concern a head line

March 15, 2017 read

**312 and counting data
breaches, in 2017, report**

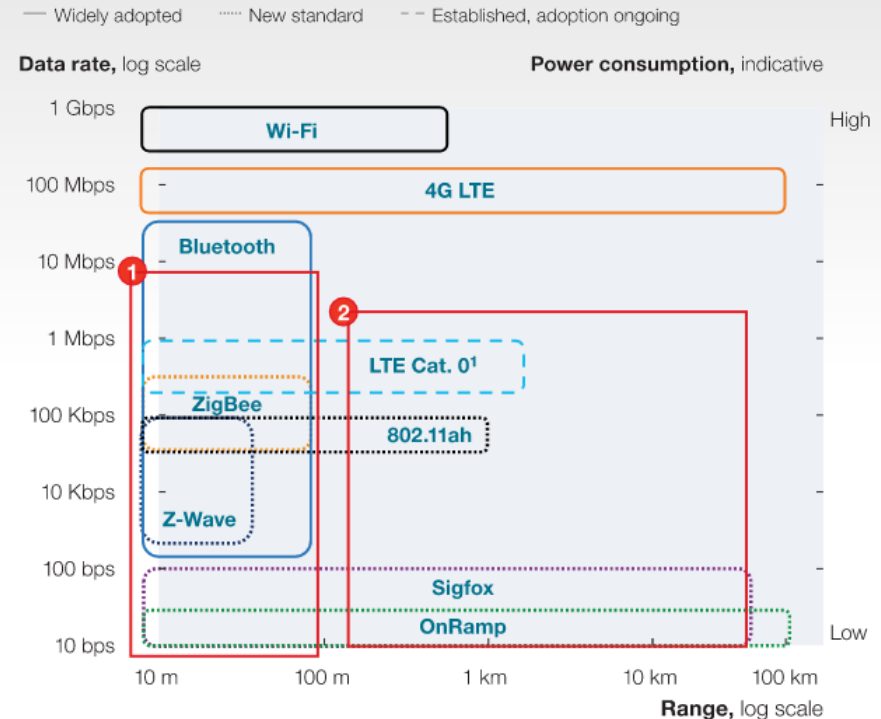
<https://www.scmagazine.com/report-finds-more-than-312-data-breaches-this-year/article/644421/>

- Cryptography, be it symmetric or asymmetric, requires a “**secret**”
- Local biometric matching please!
Assuring our security & privacy
- Securing these **secrets** is essential
- Yet the places they can be stored differ in capabilities
 - Embedded Secure Elements
 - Trusted Execution Environments
 - Trusted Processing Modules
 - White Box Encryption

Only With Standards & Certified Solutions

Can We Assure Interoperability & Proliferation

Connect objects need to be connected somehow



- ① Many competing standards for low-range, medium-low data rate hinder growth for many IoT applications
- Interoperability missing
 - Consortia wars might be emerging
 - Additional incompatibilities in higher communication layers, eg, 6LoWPAN vs ZigBee

- ② Standard white space for low-data-rate, low-power, high-range applications such as smart grid
- Wi-Fi and LTE have high power consumption
 - Alternatives with low power and wide range (eg, LTE Cat. 0, 802.11ah, Sigfox, and OnRamp) are in very early stages and compete against each other

Source McKinsey



Design the Present as the Past of the Future

What is Yours?

pa
philip andreae
and associates

Is Open For Business



www.linkedin.com/in/pandreae

Philip Andreae
Principal
Philip@Andreae.com
www.andreae.com
+1 404 680 9640



www.twitter.com/pandreae