RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: BAS-M08

A New Security Paradigm for IOT (Internet Of Threats)

Hadi Nahari

Vice President, Security CTO
Brocade Communications, Inc.
@hadinahari

#RSAC

National Academy of Engineering

Grand Challenges for 21st Century

- Make solar energy economical
- Provide energy from fusion
- Develop carbon sequestration methods
- Manage the nitrogen cycle
- Provide access to clean water
- Restore/improve urban infrastructure
- Advance health informatics
- Engineer better medicines
- Reverse-engineer the brain
- Prevent nuclear terror
- **Secure cyberspace**
- Enhance virtual reality
- Advance personalized learning
- Engineer tools of scientific discovery

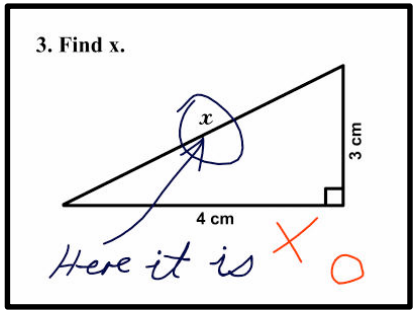
State of the Union

- Security posture compared to 2015?
  - How about compared to 2014? Or 2013?
  - …
- Poll!
- Why?

>3,000,000,000,000 threats annually

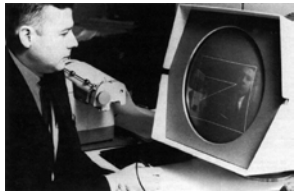
(~$110BN @$27.3/threat)

Year	2014	2015
Incidents	63,437	79,790
Breaches	1,367	2,122



Static Security

Computing: Then & Now



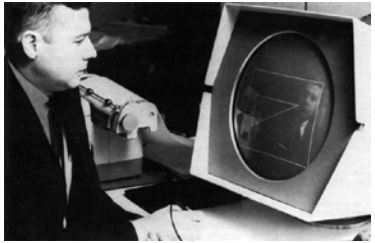





Computing has evolved tremendously

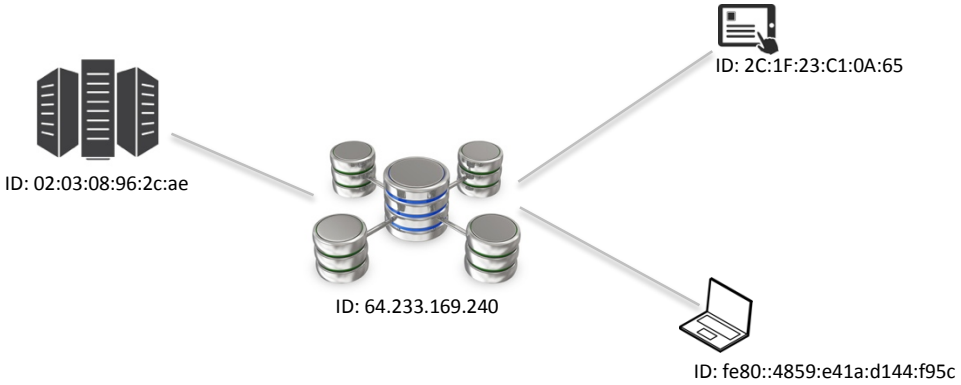
Security: Then & Now

- Old days
  - Identification, authentication, access control (ACL/MAC/DAC/...), TCB, disjointed systems, security an after-thought, etc.
- Today
  - Identification, authentication, access control (ACL/MAC/DAC/...), TCB, disjointed systems, security an after-thought, etc.
- So, security is still...



Here's Why

Machines

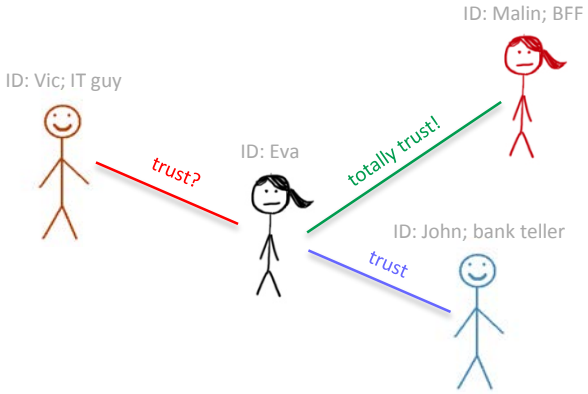


Machines rely on <u>identity</u> to interact with each other

0 1

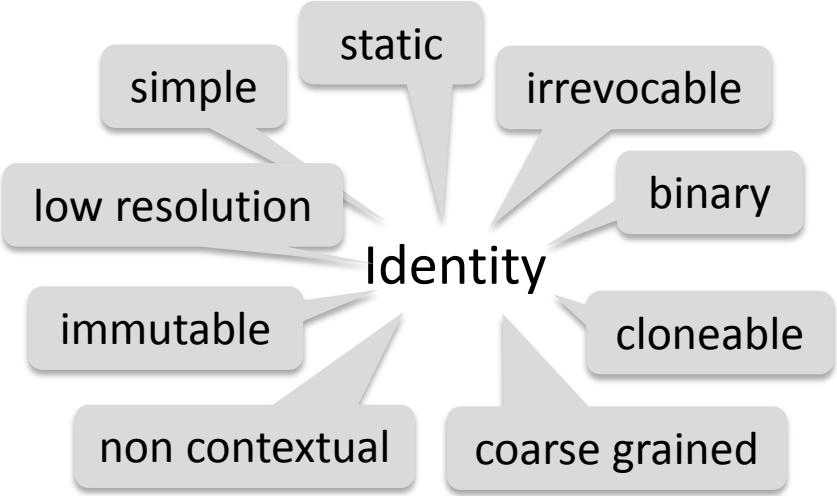
Here's Why (cont'd)

Humans



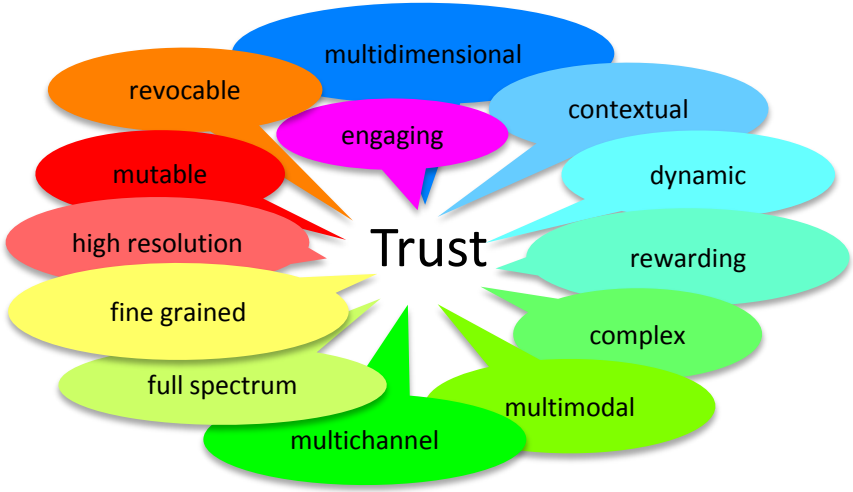
Humans, on the other hand, rely on <u>trust</u>

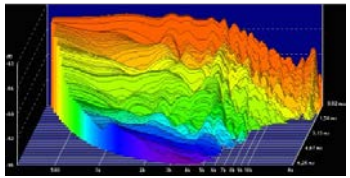
Identity vs. Trust



0	1

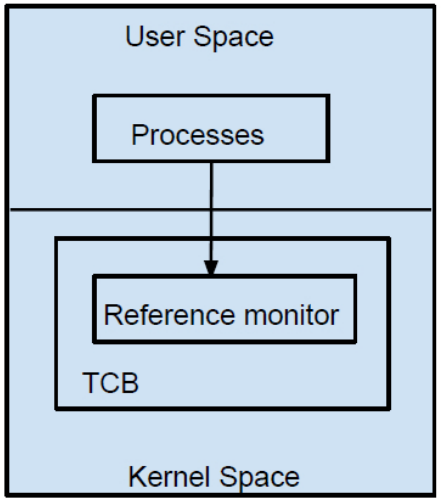
Identity vs. Trust (cont'd)

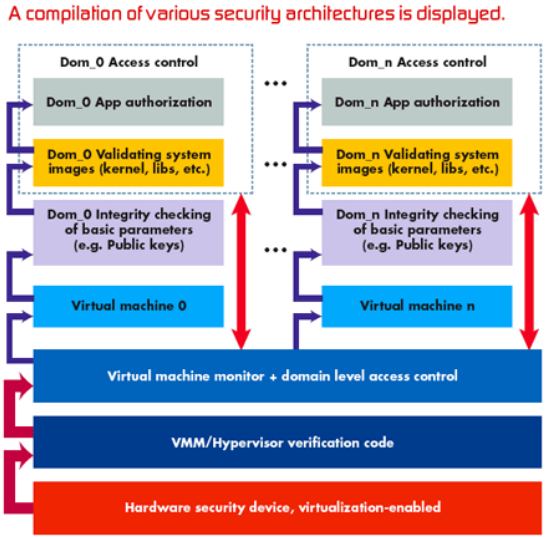




TCB, ROT, COT

In machines





Not in humans…

The Static Security Era

- Machines & humans are becoming more similar
- Issues go beyond identity vs. trust
- Static Security is presumptuous
  - Need to know adversary profile ahead of time
- Best case: just *detecting* attacks
- IMPORTANT: Static Security is not bad! still necessary
  - Just not sufficient anymore

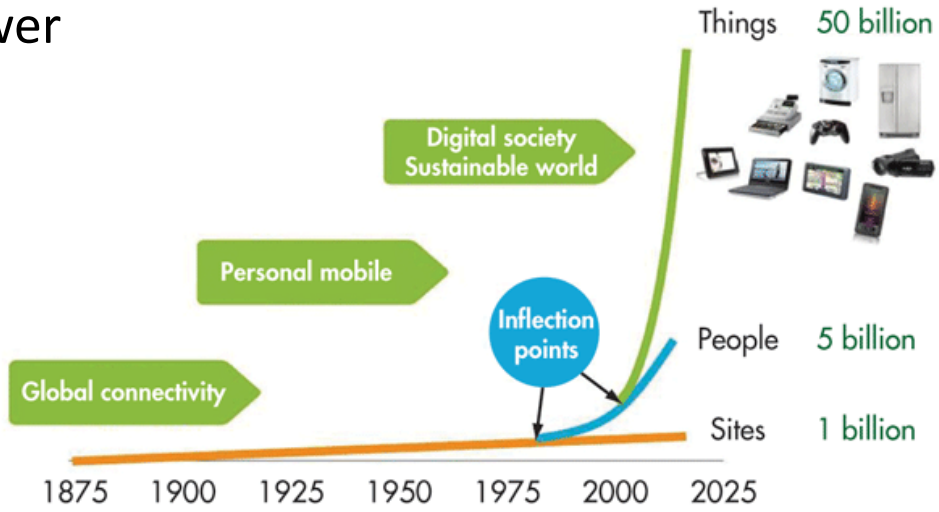
Static Security Building Blocks

- Assets, attack tree, VATA
- Identity, authentication, authorization
- Cryptography (confidentiality, integrity, authenticity, non-repudiation)
- Attestation, verification, run-/load-/crash-time integrity validation and measurement
- …

IOT 101

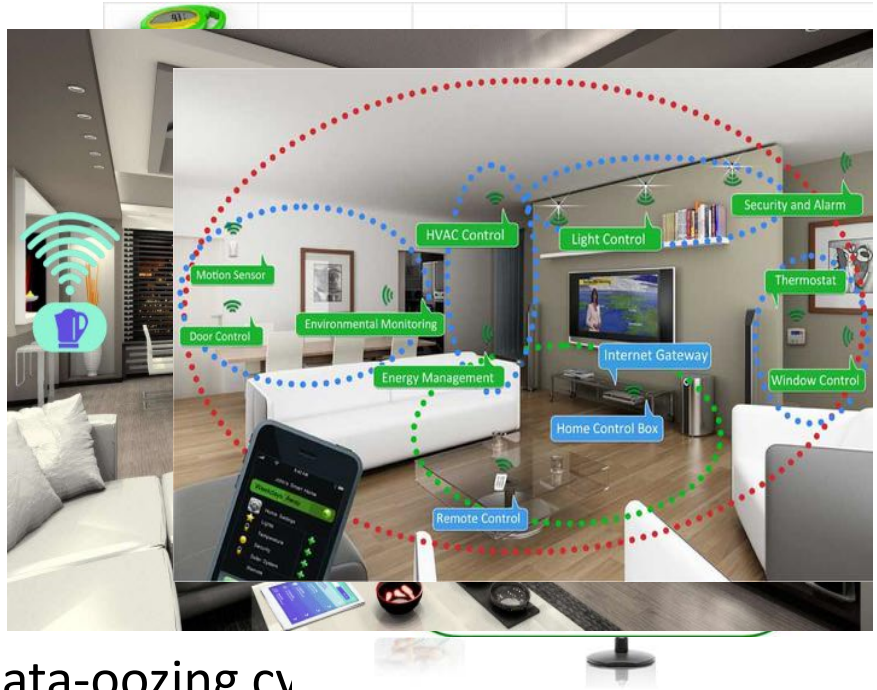
IOT Era

- What are the *Thingses* anyway?
  - Communicating data collector things with varying compute power
- What's the big deal?
  - Data generation
  - Communication
- IOT *Security*



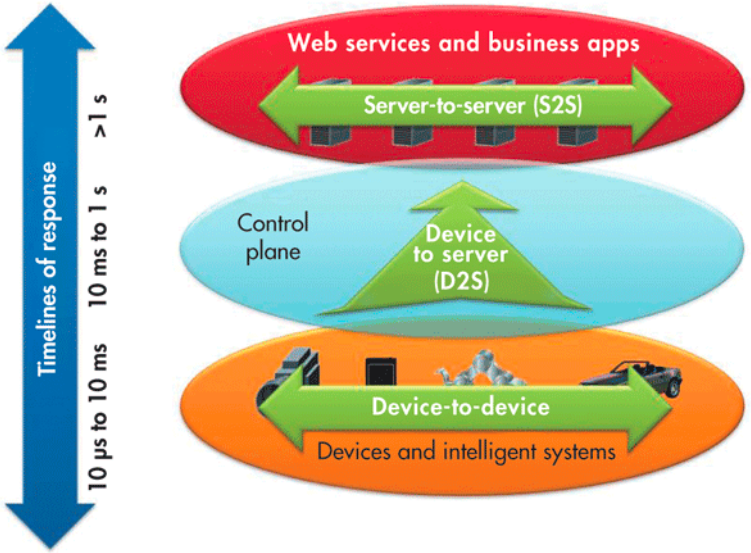
The “Thingses”

- Controllers, processors, etc. no standard comm.
- Mixed comm. (WiFi, BT, NFC, ZigBee, etc.)
- Apps & ecosystems
- Transition to services
- Massive data generation
  - We’re not just cyborgs: we’re data-oozing cy



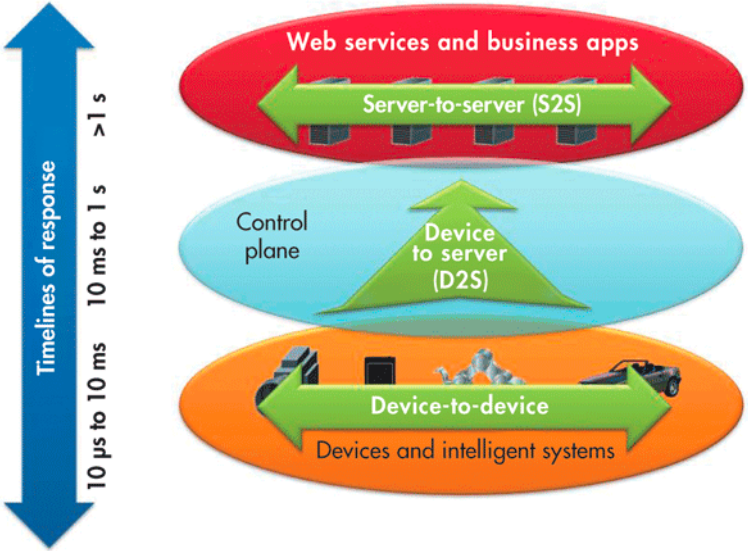
IOT Protocols

- MQTT
  - Message Queue Telemetry Transport
- MQTT-SN
  - MQTT for Sensory Networks
- XMPP
  - Extensible Messaging & Presence Transport



IOT Protocols (cont'd)

- DDS
  - Data Distribution Service
- AMQP
  - Advanced Message Queuing Protocol
- CoAP
  - Constrained Application Protocol



Observations

- IOT protocols are mainly message-based
  - The Things are (mostly) less-capable (now at least)
- Offloading processing to the backend (mainly)
  - Thus messaging & communications infrastructure
- Ergo importance of backend & data processing
  - Data volume, contextual analytics, etc.
- *Security* not the main focus of Big Data & IOT (sounds familiar?)

Result: Attackers Are Winning

- More asymmetry of the field
  - IOTs aren't really good at making good security decisions
- Easier to hack than defend (due to Static Security)
- Securing IOT end-to-end be like shooting pool with a rope

Dynamic Security

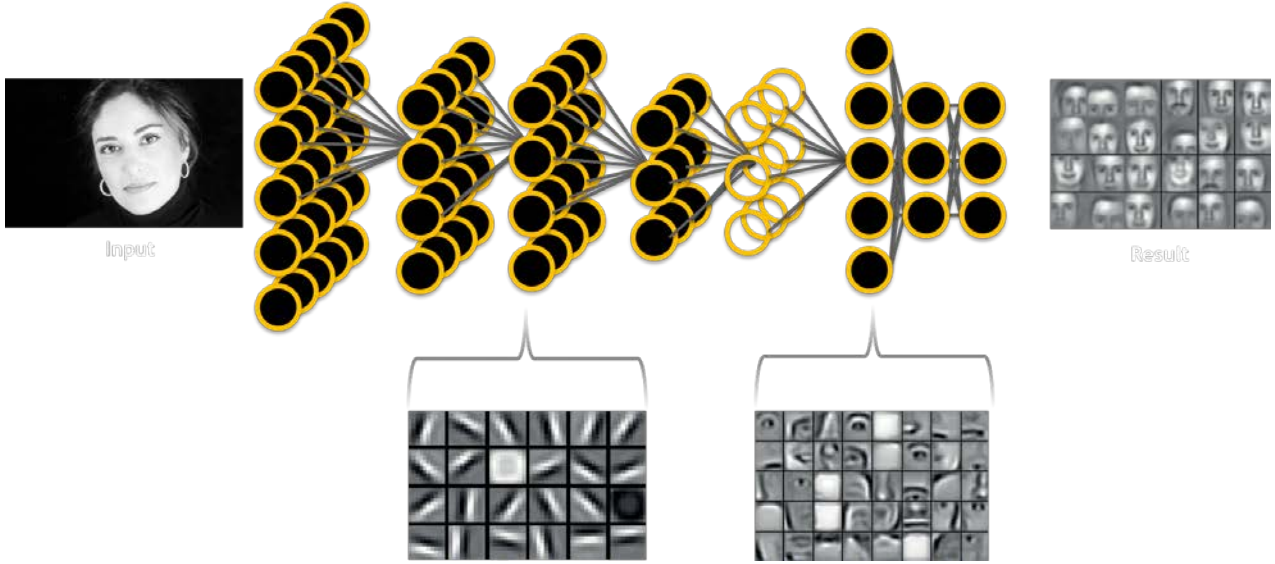
Solution: Dynamic Security

- Designing systems security according to runtime behavior
- Protocol- *and* data- *and* context-driven
- Distributed by nature
  - Processing boundaries beyond a single device
- Recency and realtime: contextual freshness matters
- Revocation abilities: leveraging comms. & backend

Dynamic Security (cont'd)

- Statistical modeling and analytics are key characteristics
- Data flows & contextual characteristics shaping security
- Behavioral modeling
  - Whose behavior? Who are the actors?
- "Learning" matters a lot to Dynamic Security

”Learning” Security → Dynamic Security



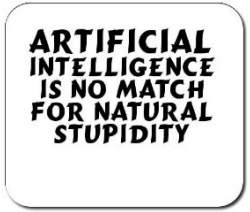
“Anything humans can do in 0.1 sec., the *right* big 10-layer ANN can do too.” *-Jeff Dean, Google*

Dynamic Security Side Effects

- Adaptive (active-defense) systems
- Self-defending (reactive-defense) systems
- Self-organizing (proactive) systems
- By applying predictive-modeling & AI
  - We should *predict* anomalous behavior, not just detect it

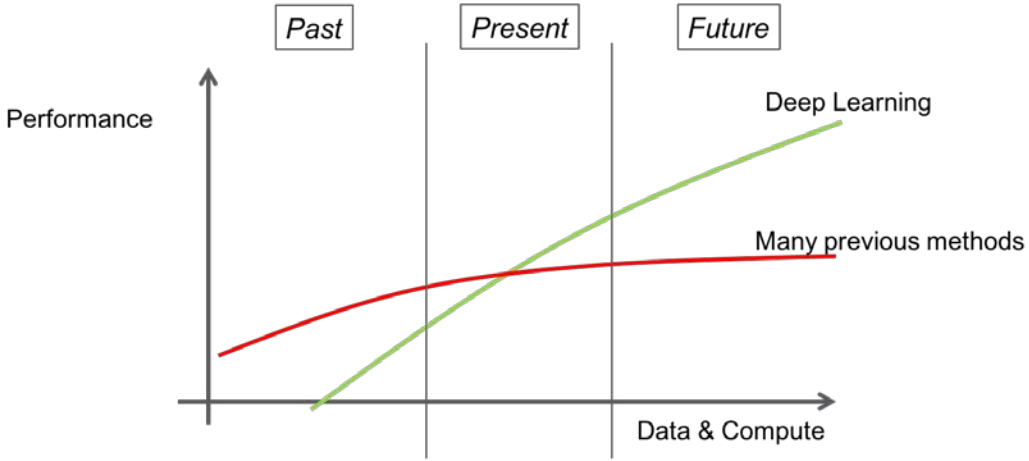
Dynamic Security Building Blocks

- AI
- AI + Big Data + Analytics
- AI + Big Data + Analytics + ML/DL
- Data → Information → Actionable Intelligence
  - *Action* is the next big thing
  - Professor Karl Friston, University College London
  - "Order of Magnitude Labs", etc.



Dynamic Security and Data

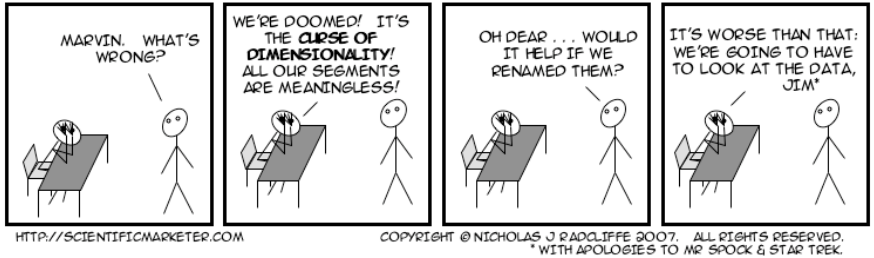
- Dynamic Security *in theory* improves with scale
- IOT = more data



Slide courtesy of Adam Coates, Baidu Research

Challenges

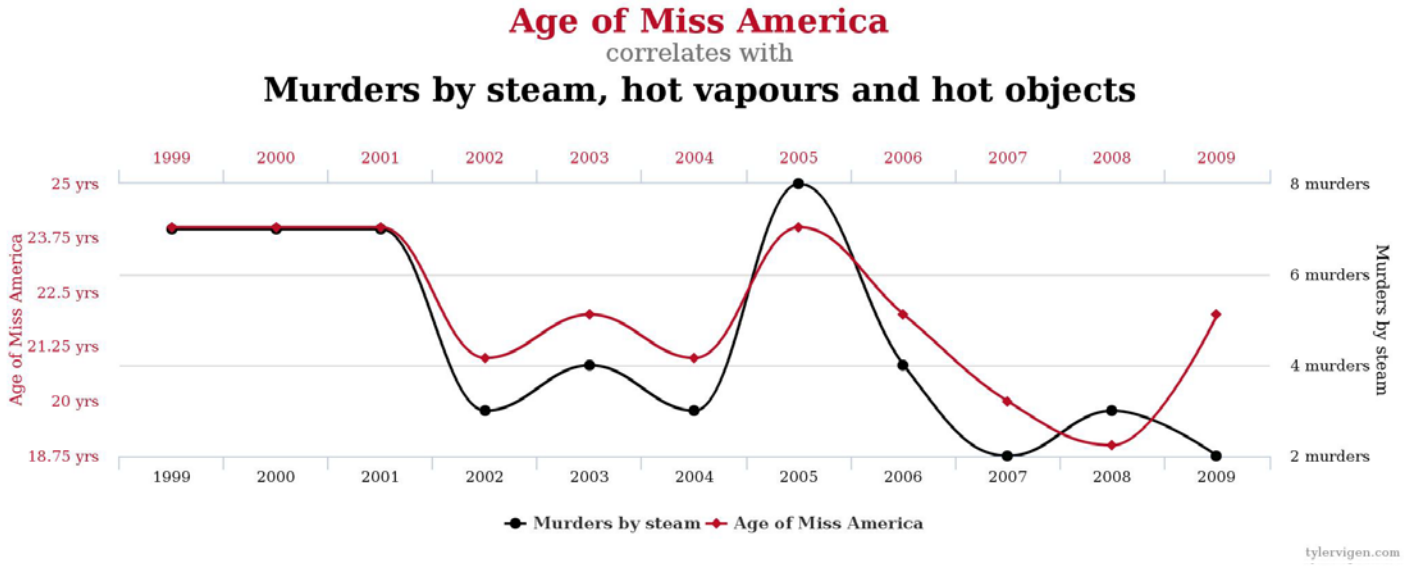
- Baselining
  - Curse of dimensionality
- Requires cooperating systems
  - Among mutually-distrusting actors
- Privacy
  - Data sharing: digital equivalent of cognitive dissonance
  - DataHub @MIT CSAIL: very promising project
    - Sandy Pentland, Thomas Hardjono, et al.



Challenges (cont'd)

- simple correlations
- statistical significance

P-VALUE	INTERPRETATION
0.001	HIGHLY SIGNIFICANT
0.01	
0.02	



Conclusion

Summary

- Static Security has already reached its limits
- Dynamic Security is the natural next step
- Prerequisite technologies exist
  - Big challenge is composing a cooperative flow
  - Both on business and technical fronts
- Until and unless Dynamic Security is the norm, hackers win
- Static Security will still be required for the foreseeable future

Apply

- You have entered IOT whether or not you know it
- Identify which security is your reference: Static or Dynamic?
  - Follow the data and who processes it
  - Do you need to know the attack vector ahead of the time?
- Start creating data models to reason about your system security
- Do not throw away Static Security measures
  - Augment them by Dynamic Security

Thank You!

http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470624469.html

Hadi Nahari
hadi.nahari@gmail.com
hadinahari