Exceptional service in the national interest

Sandia National Laboratories

Trustworthy Design Architecture: Cyber-Physical System

Peter Choi, PhD, CISSP, CSSLP – Sandia National Laboratories
Adrian Chavez – Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

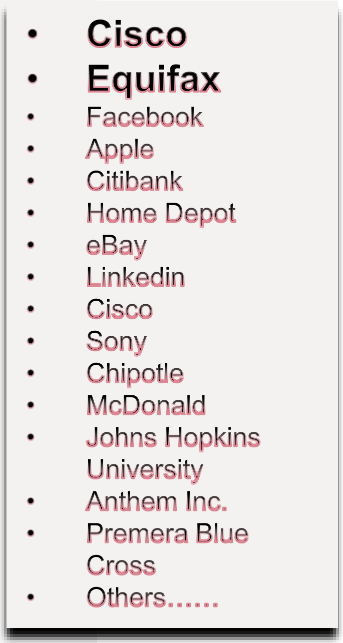
NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

We (Information Era Security) really Tried…

Cybersecurity, Are we there yet?

- **Information “insecurity”**
  - OPM
  - IRS
  - Lockheed Martin Corporation
  - Boeing
  - Amazon
  - Yahoo
  - Target
  - Ashley Madison
  - JP Morgan
  - HBO
  - Hilton Hotel
  - etc.



- **Cisco**
- **Equifax**
- Facebook
- Apple
- Citibank
- Home Depot
- eBay
- Linkedin
- Cisco
- Sony
- Chipotle
- McDonald
- Johns Hopkins University
- Anthem Inc.
- Premera Blue Cross
- Others.......

“There are two types of companies: those that have been hacked, and those who don't know they have been hacked.”

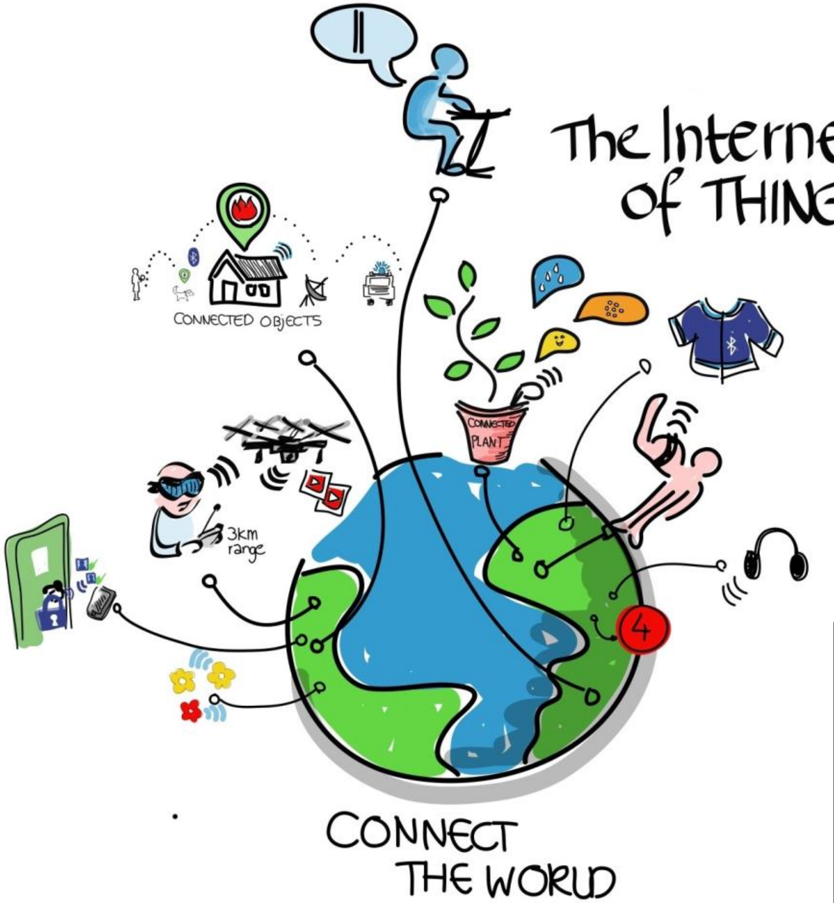
- John Chambers

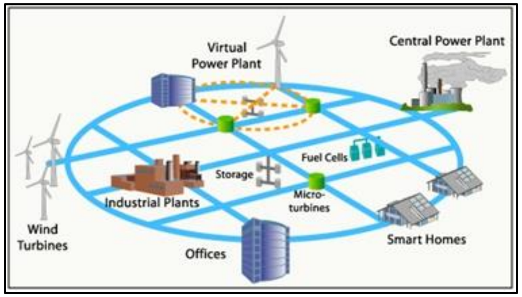
But Despite of this cyber insecurity…
Internet is Thriving!

Information Age…What is at stake?

- Personally Identifiable Information (PII) - Privacy
- Intellectual Properties, national secrets
- Credit cards and bank accounts

Information Age → Cyber-Physical Age



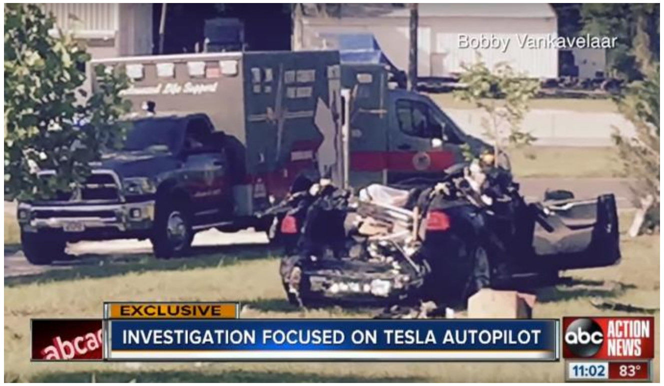


Can we afford to trust technology blindly?

Ex-Navy SEAL who died when his self-driving car crashed into a truck

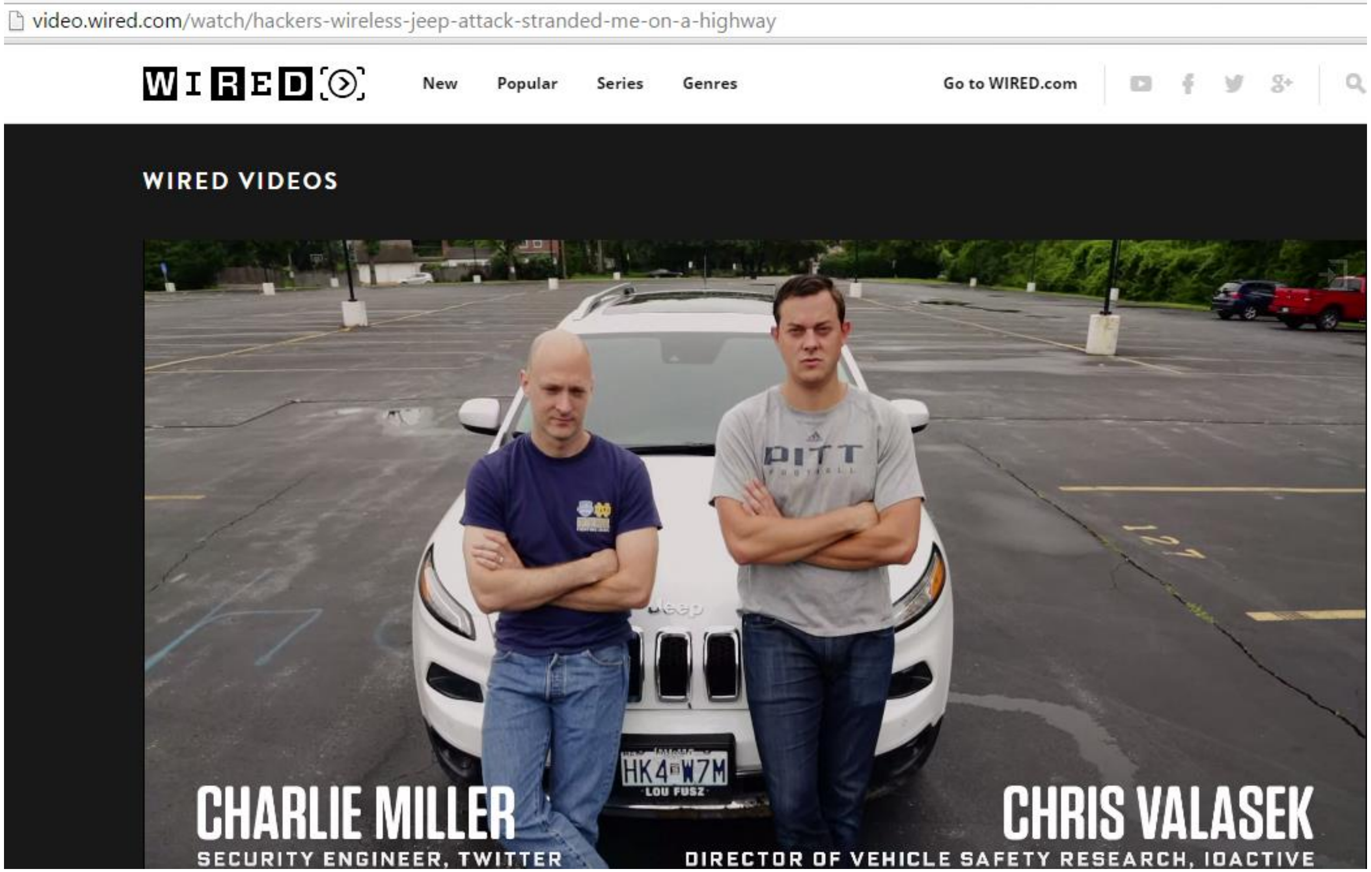
Joshua Brown, 40, died after his computer-guided Tesla Model S plowed into a tractor trailer on a freeway in Williston, Florida.

*Photo from Daily Mail



Did you know that most modern cars you drive….

- Have ~100 ECUs in them - ~100 miniature computers
- Over 100 million lines of code/car



video.wired.com/watch/hackers-wireless-jeep-attack-stranded-me-on-a-highway

WIRED VIDEOS

CHARLIE MILLER
SECURITY ENGINEER, TWITTER

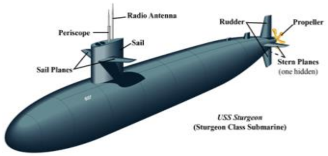
CHRIS VALASEK
DIRECTOR OF VEHICLE SAFETY RESEARCH, IOACTIVE

What is really at stake in Cyber-Physical World?

Information Age	“Cyber-Physical Age”
Propaganda	Critical Infrastructure
Disruption to information, theft of intellectual property (i.e., Sony) and money	Disruption to critical infrastructure service, can result in significant loss of lives and physical assets
Terrorism enabled by moving “electrons”	Terrorism enabled by moving physical masses - “cyber jihad” with airplanes, cars, and robots

Cyber-Physical Age

Information Age



Cyber-Physical Age

Information Age

Cybersecurity Problems

Cyber-Physical System

Revolutionary Security Solution is Needed for CPS

Information Security Solutions	Information Era Attributes	Cyber-Physical System Attributes
Virus Checking	Needs continuous update from external sources	Limited computing resources and network connection
IDS/IPS & Firewall	Continuous updates needed, unavailable and expensive SMEs are needed	Deterministic physical behavior, reliable timing responses, unsuitable for 24/7 operational environment of ICS
Patch Management	Needs external source support, operational acceptance test	Deterministic physical behavior, reliable timing responses, unsuitable for 24/7 operational environment of ICS
Confidentiality/ Encryption	Secret is exposed every time ID is compared	Authenticity and integrity of messaging is needed, hardware identities cannot be spoofed and ID must be viewed every time

Are there cybersecurity solution/s that avoids having to rely on *virus* and *patch* updates, *IDS/IPS SMEs*, and the *stronger digital authentication* schema?

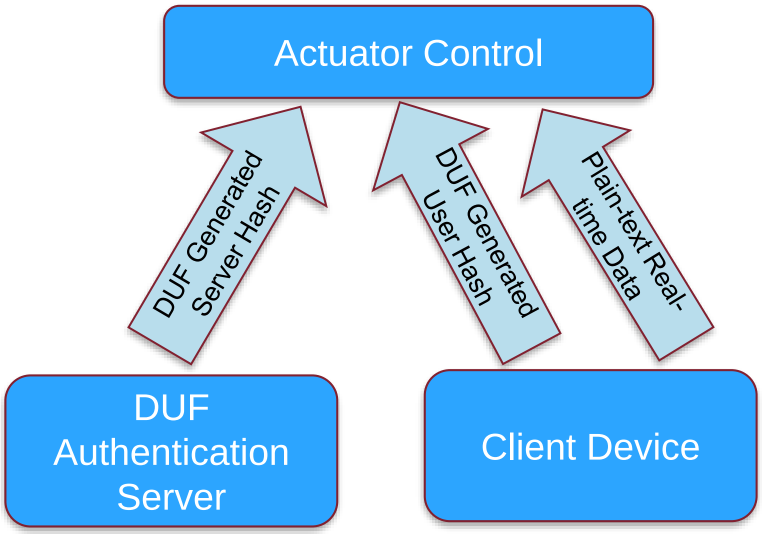
One Possible Solution for CPS: Trustworthy Design Architecture

- **Trustworthy Design Architecture (TDA)**
  - Uses sessionless, digitally unclonable authentication protocol (IEEE 2015 Mobile Services Conference) – Digitally Unclonable Function (DUF) protocol
  - Security built exclusively on “self-contained, white listed” rules
  - Digital commands and sensor data, validated via physical behavior
- **TDA Prototype Models**
  - Built Access Control System prototype using DUF protocol (Summer of 2016)
  - Improvement on “card not present” EMV transaction
  - Unclonable, unspoofable remote key fob for automobiles and garage door opener
  - Unspoofable Smartmeter
  - Etc.

DUF Access Control System Prototype

Prototype contained three main software:

- DUF Server
- DUF Registration Client
- DUF Access Agent



Actuator Control

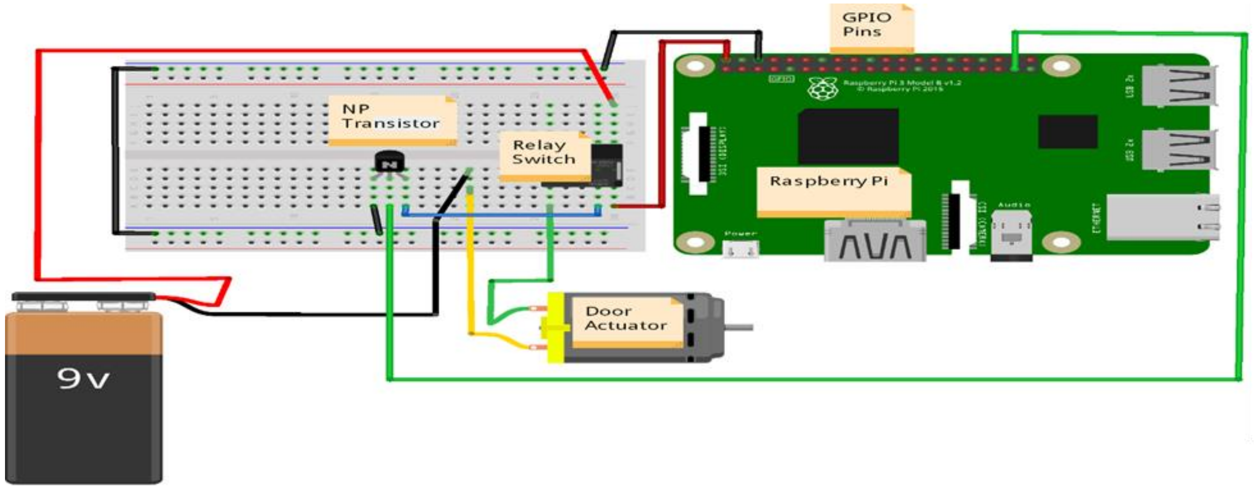
DUF Generated Server Hash

DUF Generated User Hash

Plain-text Real-time Data

DUF Authentication Server

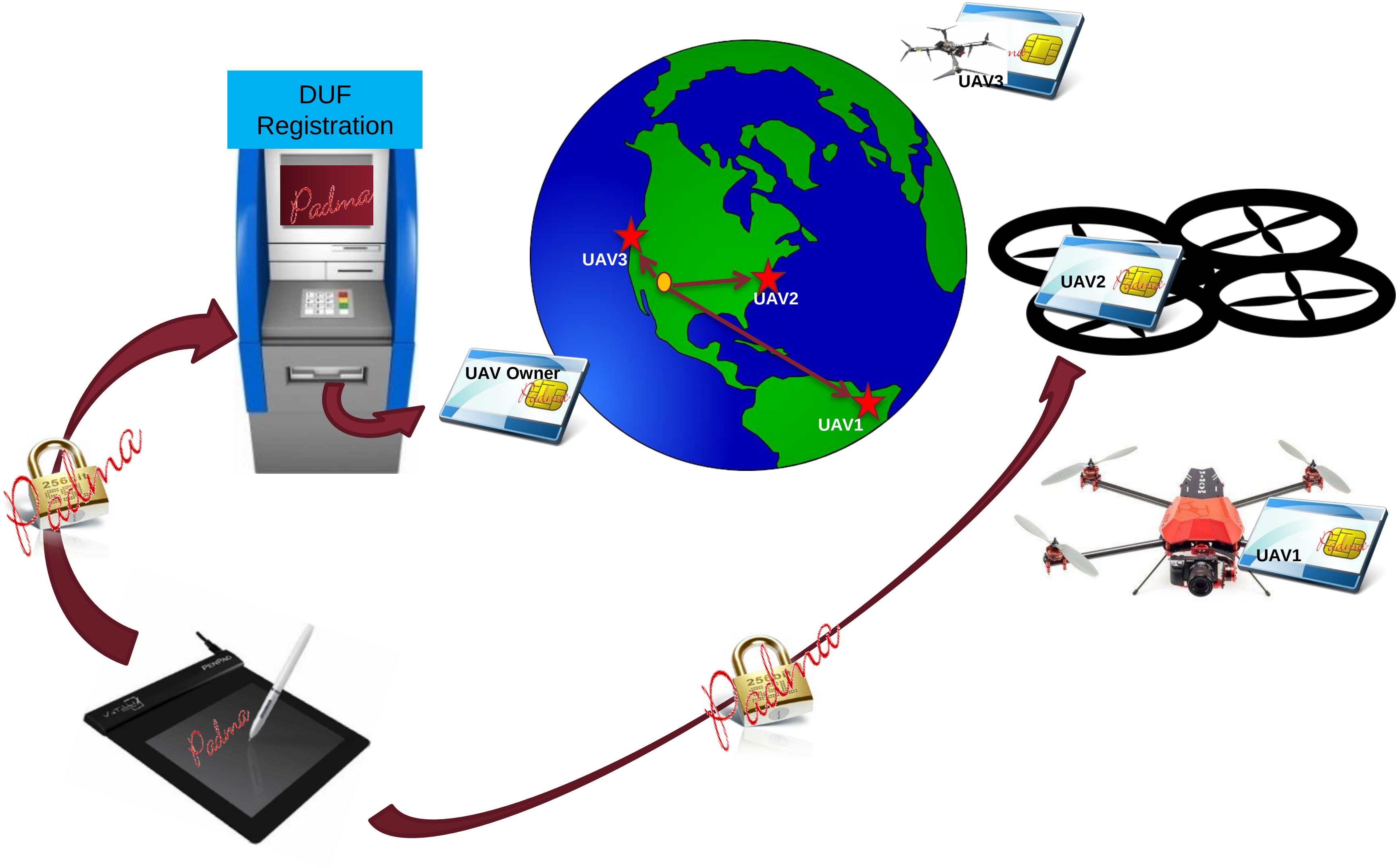
Client Device



DUF Access Control System (Continued)

- **Lessons learned**
  - For simple “open/lock” command to process DUF command, we needed to install 3.5 million lines of Linux kernel code ➔ demonstrates utility of using “white list” rule
  - “Red Team” analysis is needed to prove security of “maintenance free” TDA architecture
  - Can’t demonstrate scalability on the “shoe string” budget
    - Two months of college Intern at half time
    - It took 1 months to order all the parts before we can even code anything

Looking for Potential Product Dev Partnership



Questions?

Sung (Peter) Choi
schoi@sandia.gov

Attack Trend Graph from NSS-17

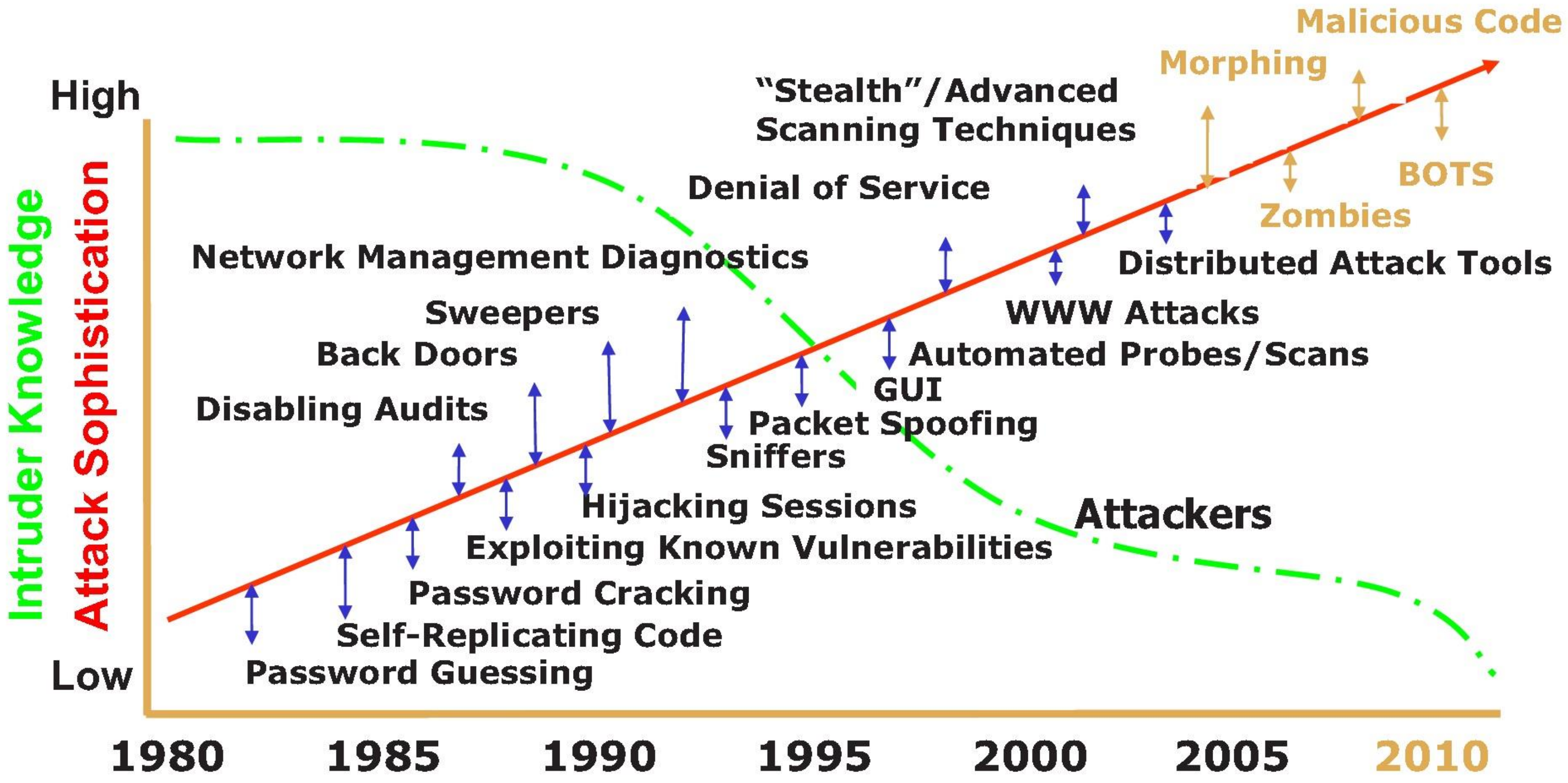
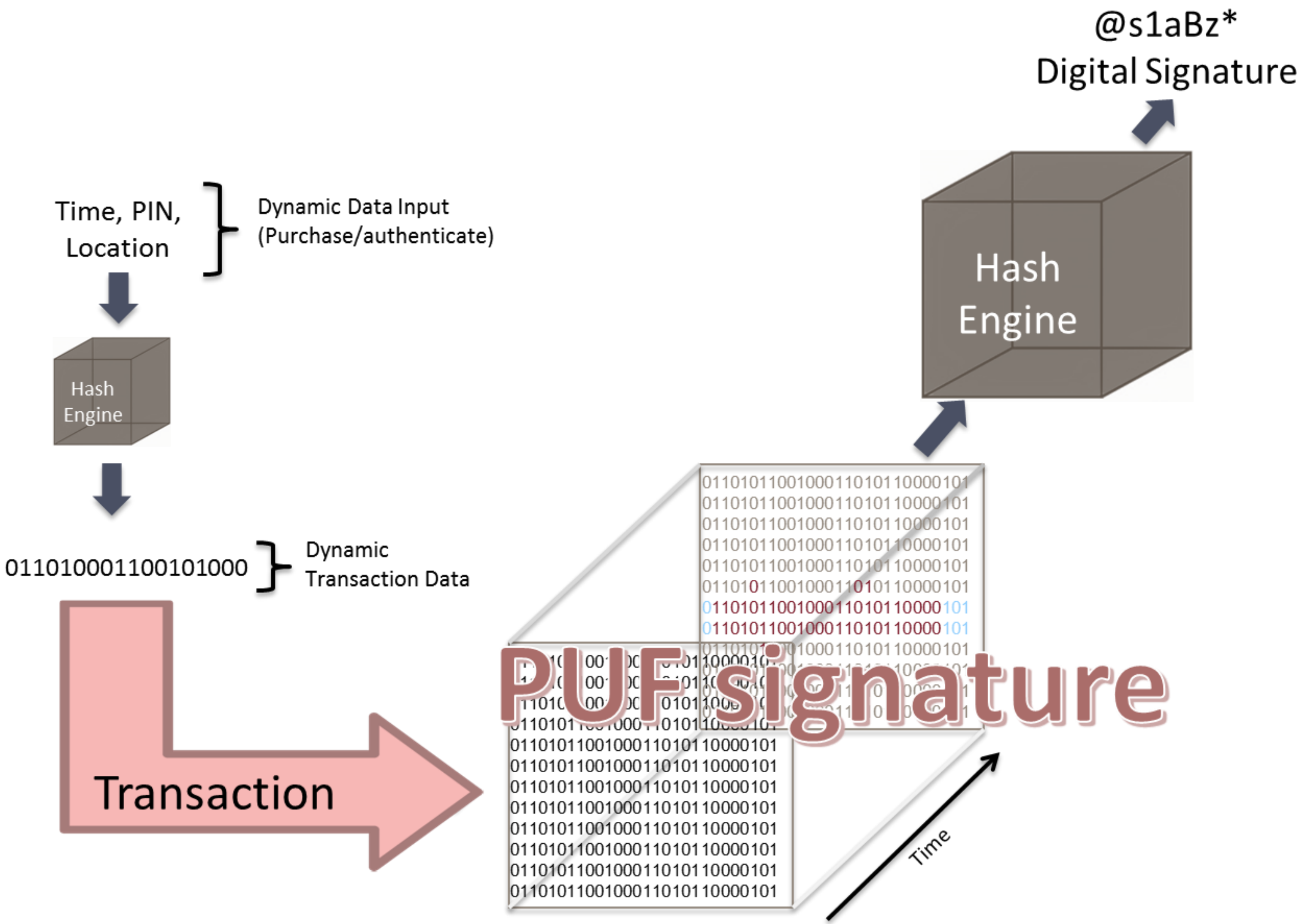


FIG. 7. The increasing complexity of threats as attackers proliferate.[4]

Why is it more secure?

Standard Authentication	DUF Authentication
Uses password or PIN to access "static data" on the secure chip	Passwords/PIN are just used as dynamic input to creating physical signature of a secured chip
Confidentiality/Encryption is used to "securely transmit" digital ID	Integrity (Hash function) is used to authenticate device and human ID
Digital ID can be replicated and processed by any generic computing device	Digital ID can only be validated by being processed through unique DUF device
Remote identity theft is rampant & completely possible (1 to many model)	Access to physical DUF device is necessary to compromise DUF identity (1 to 1 model)
Stronger authentication usually means greater inconvenience to end-users	Extremely convenient, near impossibly to spoof remotely
New multi-factor authentication requires having completely different infrastructure	Plug-in solution that integrates into existing legacy infrastructure
Identity management susceptible to insider threat	Identity management solution that addresses insider threat with technical controls

DUF Watermarking Technology



Cyber-Physical Identity Technologies

- **Sandia's US Patent Applications:**
  - Indoor Positioning System with Auto-registration (14/051,304)
  - Identity Management Using Ephemeral Biometrics (14/051,318)
  - Methods and Systems for Authenticating Identity (15/183,454)
  - Methods for Communicating Data Utilizing Sessionless Dynamic Encryption (15/286,344)