INTERNET2®

2016 TECHNOLOGY exchange

MIAMI FL

SEPTEMBER 25–28

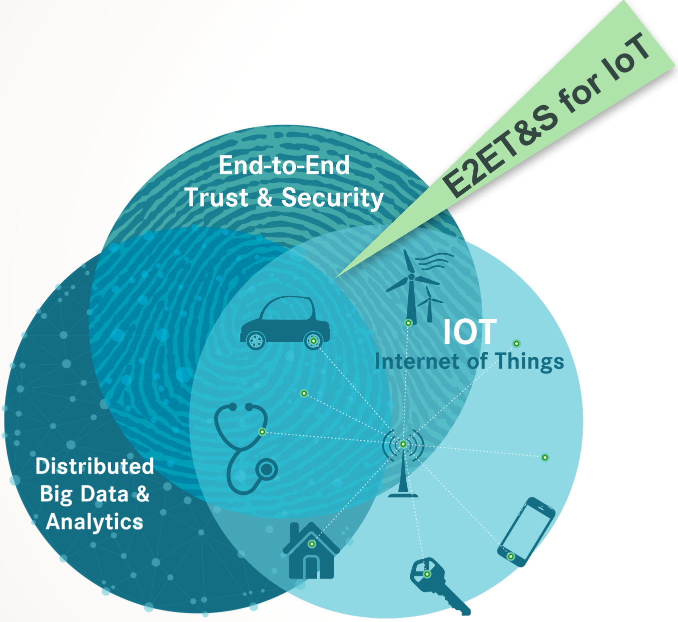
COLLABORATIVE INNOVATION COMMUNITY MEETING PART II: END-TO-END TRUST & SECURITY FOR IOT AND TIPPSS

Collaborative Innovation Community Meeting Part II: End-to-End Trust & Security for IoT and TIPPSS

CONTENTS

- **End-to-End Trust & Security for IoT:** *Florence Hudson, Internet2*
- **Importance of Trust, Identity, Privacy, Protection, Safety & Security (TIPPSS):** *Mark Cather, UMBC*
- **A Few Usually Suspect Thoughts:** *Ken Klingenstein, Internet2*
- **Panel Discussion: Where Do We Go Next? How Do We Make it Real?:** *Mark Cather, UMBC, Ken Klingenstein, Internet2, Scot Ransbottom, Virginia Tech*
- **Recommended Next Steps:** *Florence Hudson, Internet2*

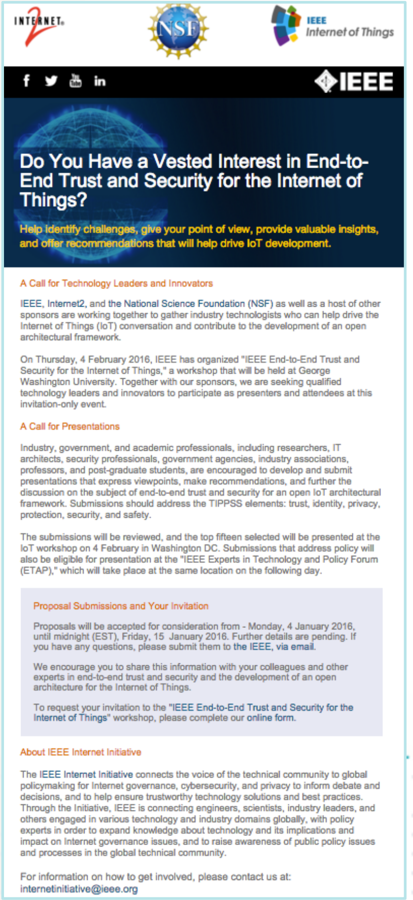
Collaborative Innovation Community Working Groups are exploring future, strategic innovations in advanced networking and trust & identity for the research and education community.



E2ET&S for IoT: A recommended implementation approach to enable future "End-to-End Trust & Security" innovations

Addressing trust, identity, privacy, physical & cyber security, compliance, etc. of people, devices, data, and the network

End-to-end Trust & Security for IoT Workshop, February 4, 2016, developed focus on TIPPSS



Do You Have a Vested Interest in End-to-End Trust and Security for the Internet of Things?

Help identify challenges, give your point of view, provide valuable insights, and offer recommendations that will help drive IoT development.

A Call for Technology Leaders and Innovators

IEEE, Internet2, and the National Science Foundation (NSF) as well as a host of other sponsors are working together to gather industry technologists who can help drive the Internet of Things (IoT) conversation and contribute to the development of an open architectural framework.

On Thursday, 4 February 2016, IEEE has organized "IEEE End-to-End Trust and Security for the Internet of Things," a workshop that will be held at George Washington University. Together with our sponsors, we are seeking qualified technology leaders and innovators to participate as presenters and attendees at this invitation-only event.

A Call for Presentations

Industry, government, and academic professionals, including researchers, IT architects, security professionals, government agencies, industry associations, professors, and post-graduate students, are encouraged to develop and submit presentations that express viewpoints, make recommendations, and further the discussion on the subject of end-to-end trust and security for an open IoT architectural framework. Submissions should address the TIPPSS elements: trust, identity, privacy, protection, security, and safety.

The submissions will be reviewed, and the top fifteen selected will be presented at the IoT workshop on 4 February in Washington DC. Submissions that address policy will also be eligible for presentation at the "IEEE Experts in Technology and Policy Forum (ETAP)," which will take place at the same location on the following day.

Proposal Submissions and Your Invitation

Proposals will be accepted for consideration from - Monday, 4 January 2016, until midnight (EST), Friday, 15 January 2016. Further details are pending. If you have any questions, please submit them to the IEEE, via email.

We encourage you to share this information with your colleagues and other experts in end-to-end trust and security and the development of an open architecture for the Internet of Things.

To request your invitation to the "IEEE End-to-End Trust and Security for the Internet of Things" workshop, please complete our online form.

About IEEE Internet Initiative

The IEEE Internet Initiative connects the voice of the technical community to global policymaking for Internet governance, cybersecurity, and privacy to inform debate and decisions, and to help ensure trustworthy technology solutions and best practices. Through the Initiative, IEEE is connecting engineers, scientists, industry leaders, and others engaged in various technology and industry domains globally, with policy experts in order to expand knowledge about technology and its implications and impact on Internet governance issues, and to raise awareness of public policy issues and processes in the global technical community.

For information on how to get involved, please contact us at:
internetinitiative@ieee.org

- **Event in Washington, DC co-sponsored by Internet2, IEEE, NSF, and George Washington University**
  - Followed by IEEE Experts in Technology & Policy (ETAP) event. Final ETAP report available on the CINO Wiki (http://bit.ly/1rpQN6u)
- **150+ participants, 35+ papers presented**
- **Agenda:**
  - Opening panel with participants from the US DoE, IEEE, IIC, NSF, and M2Mi
  - Afternoon break outs on Access Control & Identity Management; Architectural Framework; Policy & Standards; and Scenarios & Use Cases
  - Focus on **TIPPSS: Trust, Identity, Privacy, Protection, Safety & Security**

Importance of TIPPSS – Trust, Identity, Privacy, Protection, Safety and Security

The Current and Future of IoT

- IoT is “the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.”[1]
- IoT devices are considered a somewhat new issue, but they have been around for years. 2014 - 14 billion IoT device / 2020 - 50 billion IoT devices.[2]
- IoT will allow the interconnection, monitoring, and control of everything in every environment, but no one vendor will be able to make everything. Interoperable standards will be essential.
- Every facet of a person’s life and every company on earth will be touched.

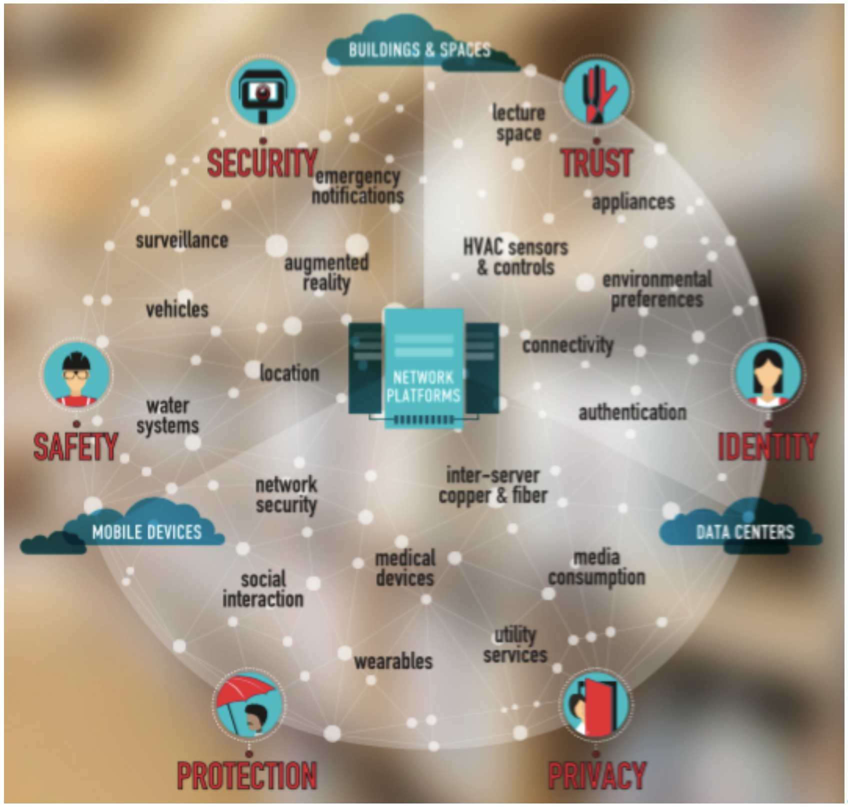
1. Gartner, “IT Glossary: Internet of Things.” June 2016.
2. Statista, “Internet of Things (IoT): Number of Connected Devices Worldwide from 2012 to 2020.” 2016.

IoT will be integrated all around us

- Building Technologies
  - Lighting Control
  - Temperature Control
  - Building Security
- Personal Area Network Technologies
  - Heads Up Displays
  - Enhanced Hearing
  - Networked Clothing
- Health Technologies
  - Activity / Exercise Monitors
  - Pacemakers
  - Insulin Pumps
  - Heart Monitors
- Municipal Technologies
  - Waste Management
  - Utility Metering, Monitoring, & Control
  - Traffic Management
- Customer Technology Interaction
  - Monitoring of Customer Behavior
  - Customer Safety
  - Wayfinding
  - Consumer Product Monitoring and Ordering
- Vehicle Technology
  - Self-driving Cars
  - Driver Assistance Technologies
  - Vehicle / Driver Integration

Addressing TIPPSS is essential to achieve wide IoT adoption

Trust
Identity
Privacy
Protection
Safety
Security



Across elements of connected ecosystem:

- Users
- Devices
- Gateways
- Communications
- Clouds
- Software
- Services
- Data
- Hardware
- Firmware

TIPPSS

- **Trust** – Trust will be essential for the adoption of IoT by consumers and enterprises. Without trust, the IoT market will not take off.
- **Identity** – Identity in an IoT context takes on many forms. Verification of the identities of people and devices will be essential.
- **Privacy** – Tremendous amounts of data will be available through the IoT. Consumers and Enterprises will need to have an understanding of how private their IoT data will remain.
- **Protection & Safety** – Safeguards are essential in protecting consumers and enterprises from physical harm where IoT devices interact with physical environments.
- **Security** – Security relates to how the devices and their related data will remain secure from confidentiality, integrity, and availability breaches.

IoT Considerations to Support TIPPSS

Data Movement Challenges

- The depth of the IoT will make the control of data movement very challenging.
  - Vendors of Vendors and Things of Things.
- Vendors will need to be transparent with customers to generate trust in products.
- Customers will need to have ownership over their data to support trust.
- Devices will communicate over whatever network is available: landline, cellular, wifi, public wifi, home networks. Trust and Security needs to be built into the communications protocols, not the transport systems.
- IoT devices will need to be able to securely communicate with each other while connected to the global internet and while isolated. Communication and authentication protocols must be developed that will allow open, secure communications.

IoT Device Security Challenges

- Tagging and Grouping
  - Device Type, Manufacturer, Model, Location, Owner, Group Affiliations, and Place of Employment
- Open Multi-vendor Patching and Configuration tools will be needed.
  - People don't keep up with patching now. When they have thousands of devices, do we expect them to do better?
  - If you are a building owner with 200 lightbulbs in the building, do you want to configure and patch each one individually? Will a single vendor solution be feasible in a building?
- How will you make sure that all your lightbulbs and IoT devices are up to date and secure? How will you detect if one IoT device is misbehaving?
- Would you want to be responsible for patching someone's pacemaker?
- Who is liable to a patching problem that damages something or harms a person?

BYOD, Consent & E-Discovery

- **BYOD:** Data will be able to move freely between IoT devices based on associations within the IoT ecosystem. Device ownership and data ownership will not always match. For example, a company's data may flow from IoT devices that the company owns to personal IoT devices associated with customers, employees, and subcontractors.
- **Consent:** Data owners will need a framework to issue and revoke access to their data within the IoT. If data owners do not feel that they have control of their data, they will be hesitant to allow their data to be within the IoT.
- **E-Discovery:** As data moves globally, litigation hold requests, E-Discovery processes, and subpoenas will be difficult. Even knowing the party to contact could become be difficult. Care will be needed to ensure the standard does not permit violations of privacy and access to data in violation of constitutional and legal protections. Legal structures within the IoT will be essential as everyone's lives become connected through the IoT.

A Few Usually Suspect Thoughts

Topics

- Presentation from Alan Karp via the IEEE/NSF/I2 IoT Meeting
  - How we middleware folks think about your things
  - Kim Cameron’s Laws of Identity
- The paths to End-to-End
  - Network layer
  - Internet Identity Layer
  - IoT
- Lessons Learned from the Identity Layer

Access Control for IoT

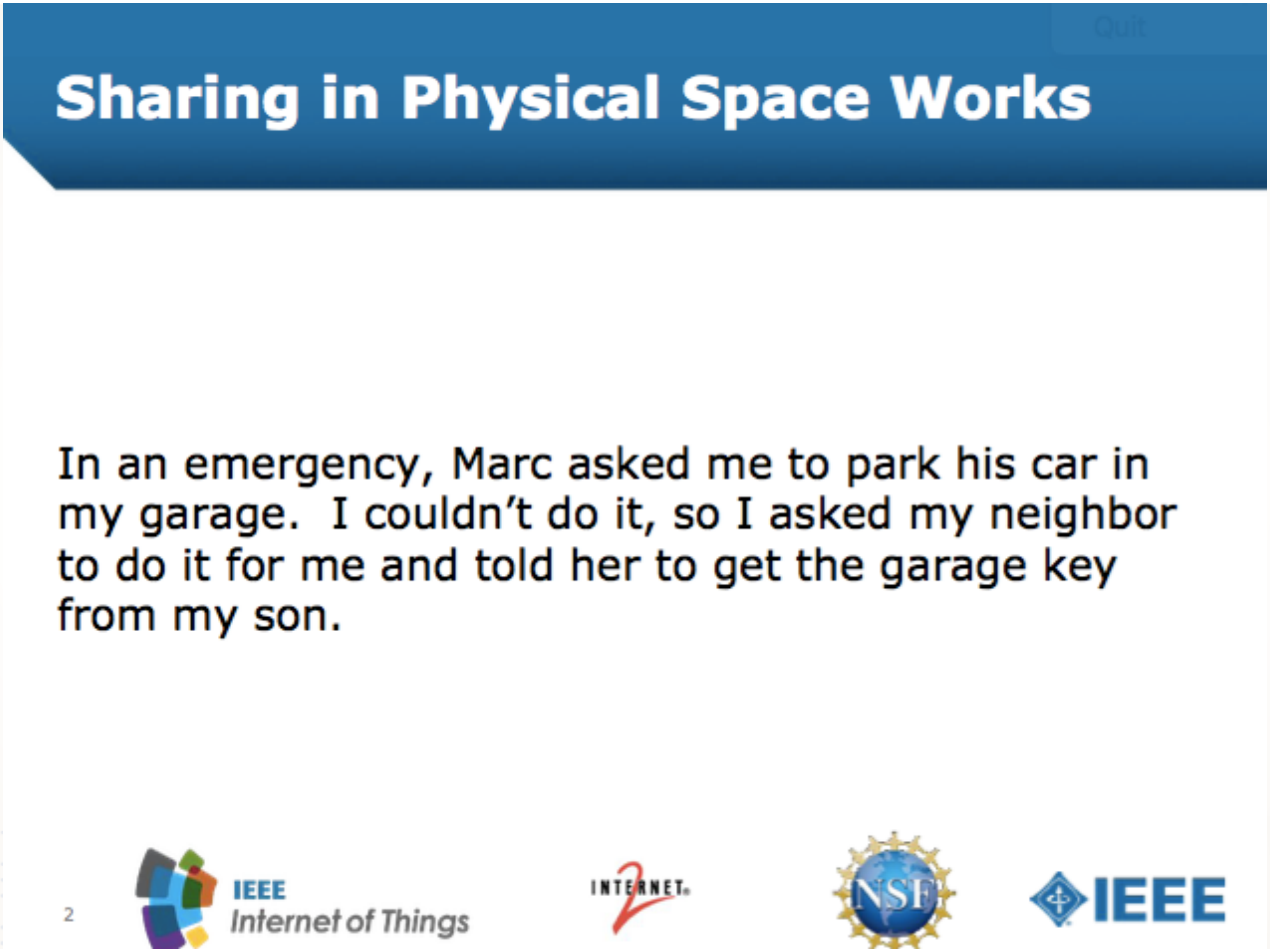
Alan H. Karp
Earth Computing
Solid Ground Beneath The Clouds

IEEE Internet of Things

INTERNET2

NSF

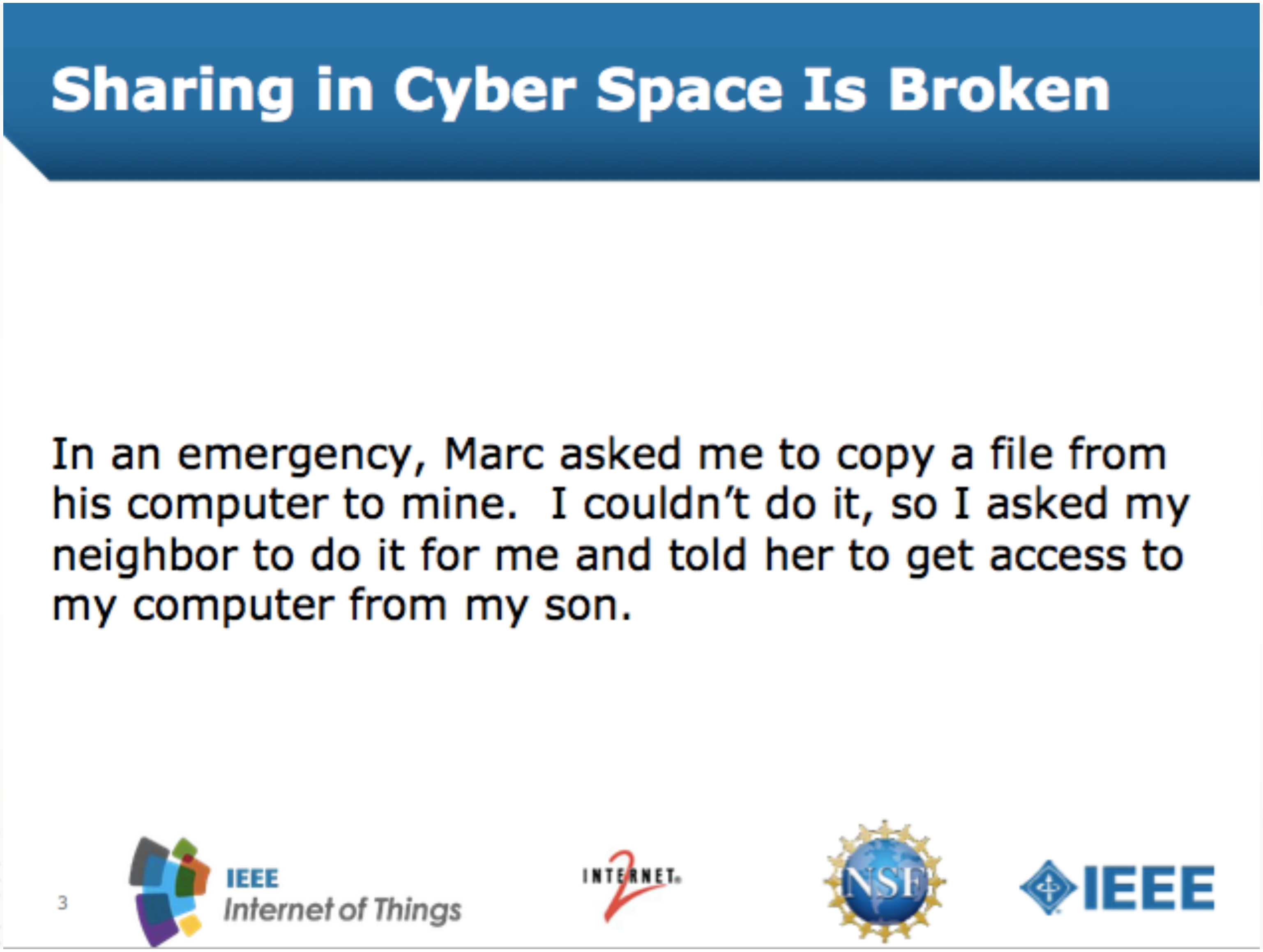
IEEE



Sharing in Physical Space Works

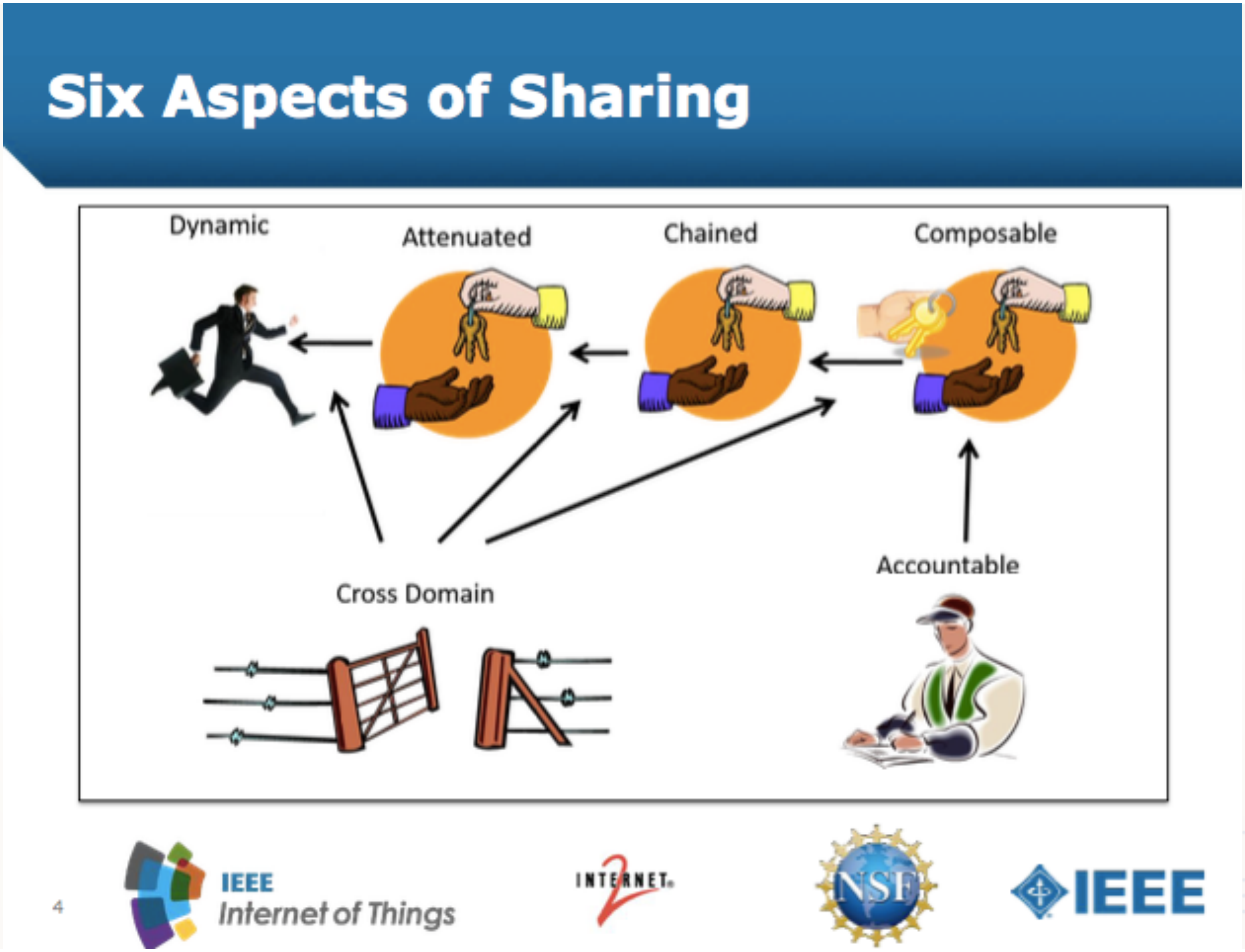
In an emergency, Marc asked me to park his car in my garage. I couldn't do it, so I asked my neighbor to do it for me and told her to get the garage key from my son.

Quit
2
IEEE Internet of Things
INTERNET2
NSF
IEEE



Sharing in Cyber Space Is Broken

In an emergency, Marc asked me to copy a file from his computer to mine. I couldn't do it, so I asked my neighbor to do it for me and told her to get access to my computer from my son.



Six Aspects of Sharing

Dynamic

Attenuated

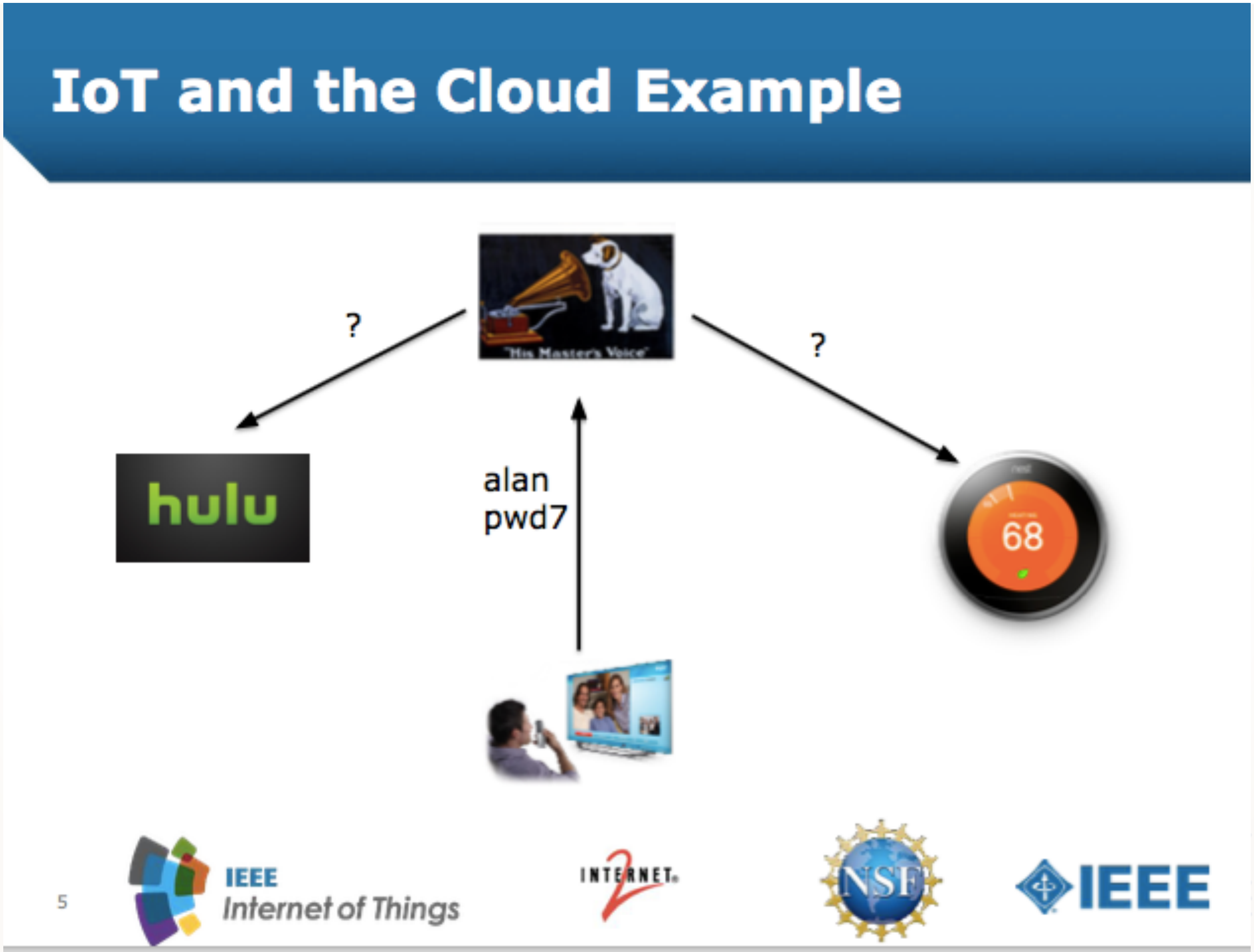
Chained

Composable

Cross Domain

Accountable

4

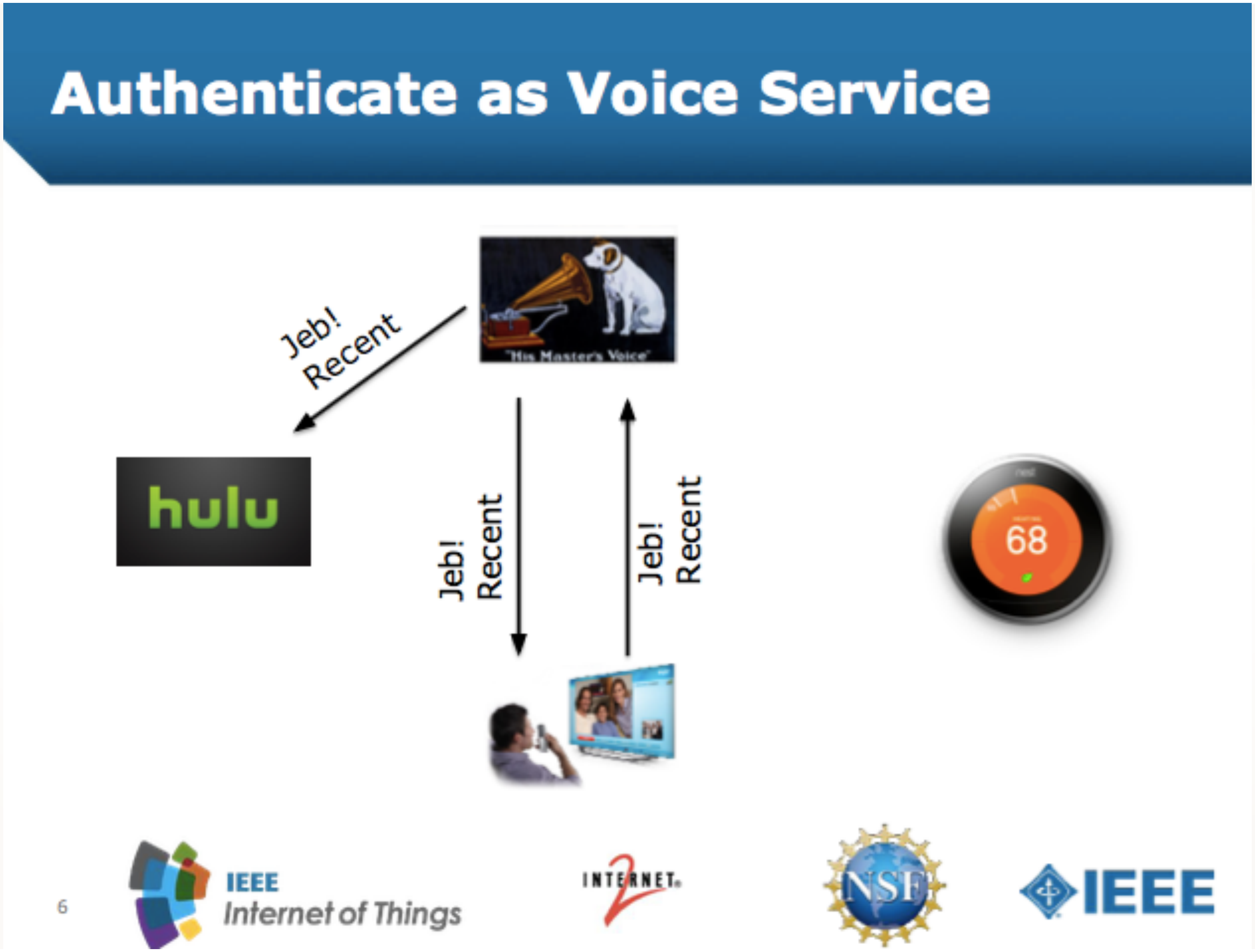


IoT and the Cloud Example

?

?

alan
pwd7



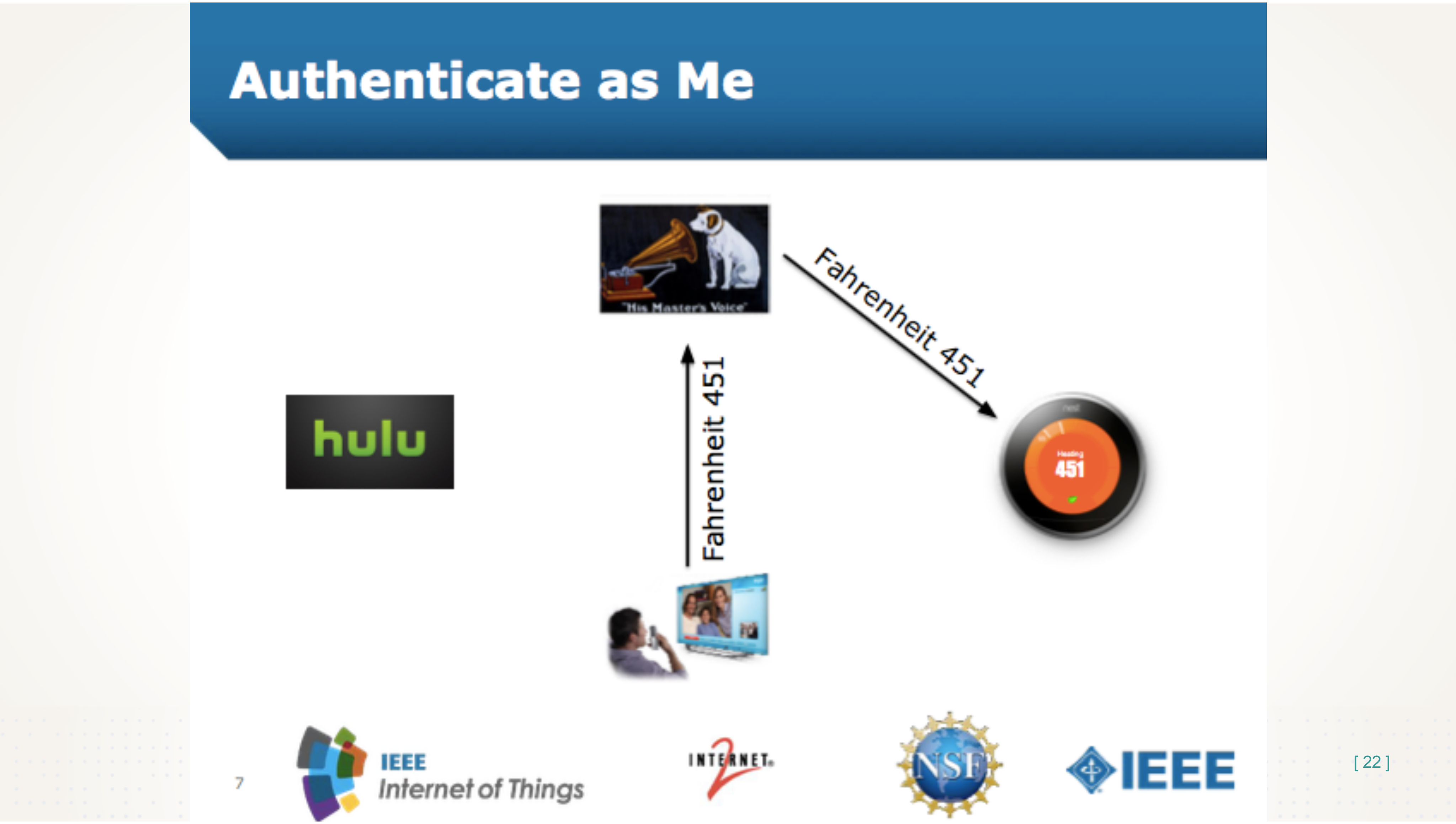
Authenticate as Voice Service

Jeb!
Recent

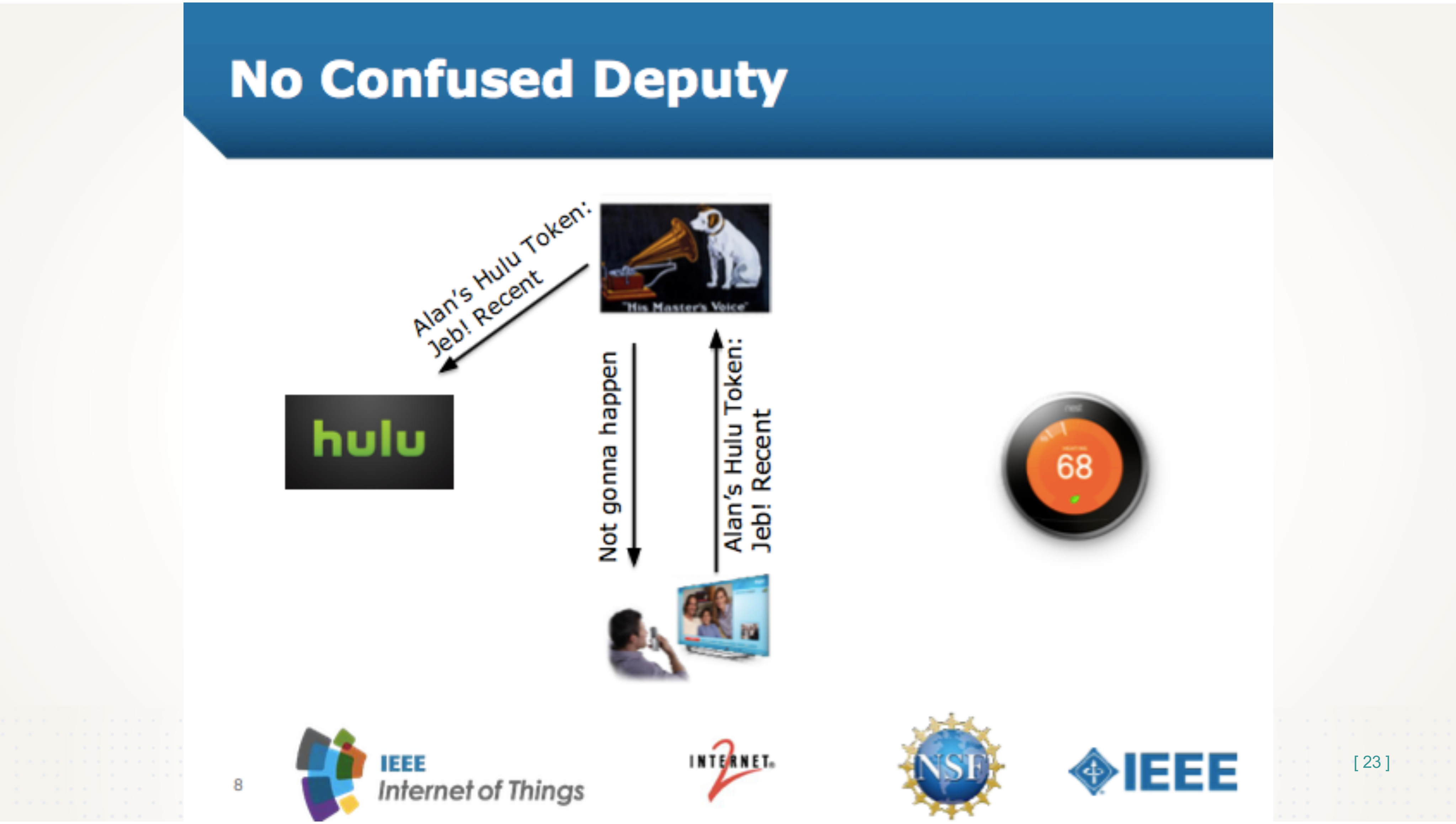
Jeb!
Recent

Jeb!
Recent

6



Authenticate as Me

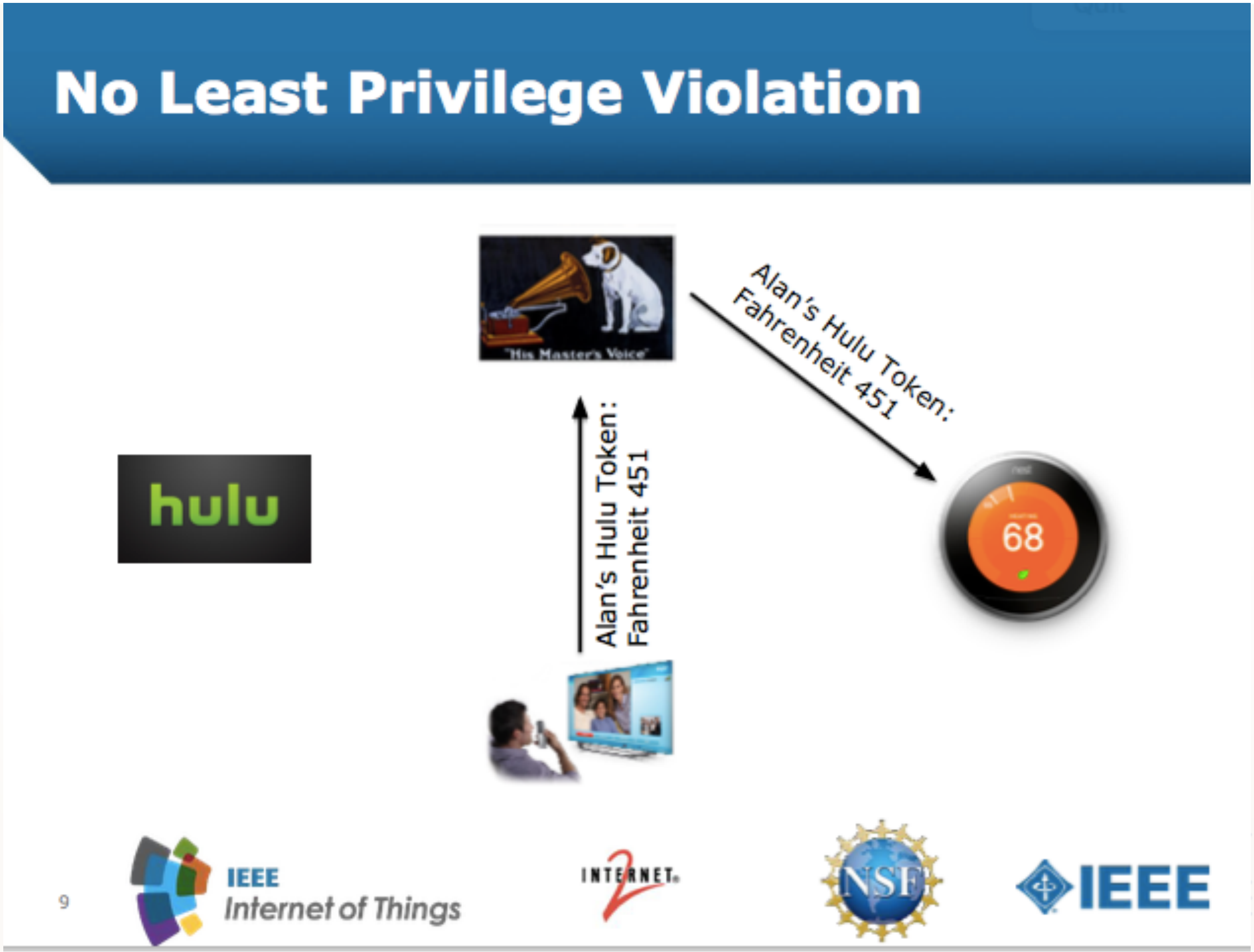


No Confused Deputy

Alan's Hulu Token:
Jeb! Recent

Not gonna happen

Alan's Hulu Token:
Jeb! Recent



No Least Privilege Violation

Alan's Hulu Token: Fahrenheit 451

Alan's Hulu Token: Fahrenheit 451

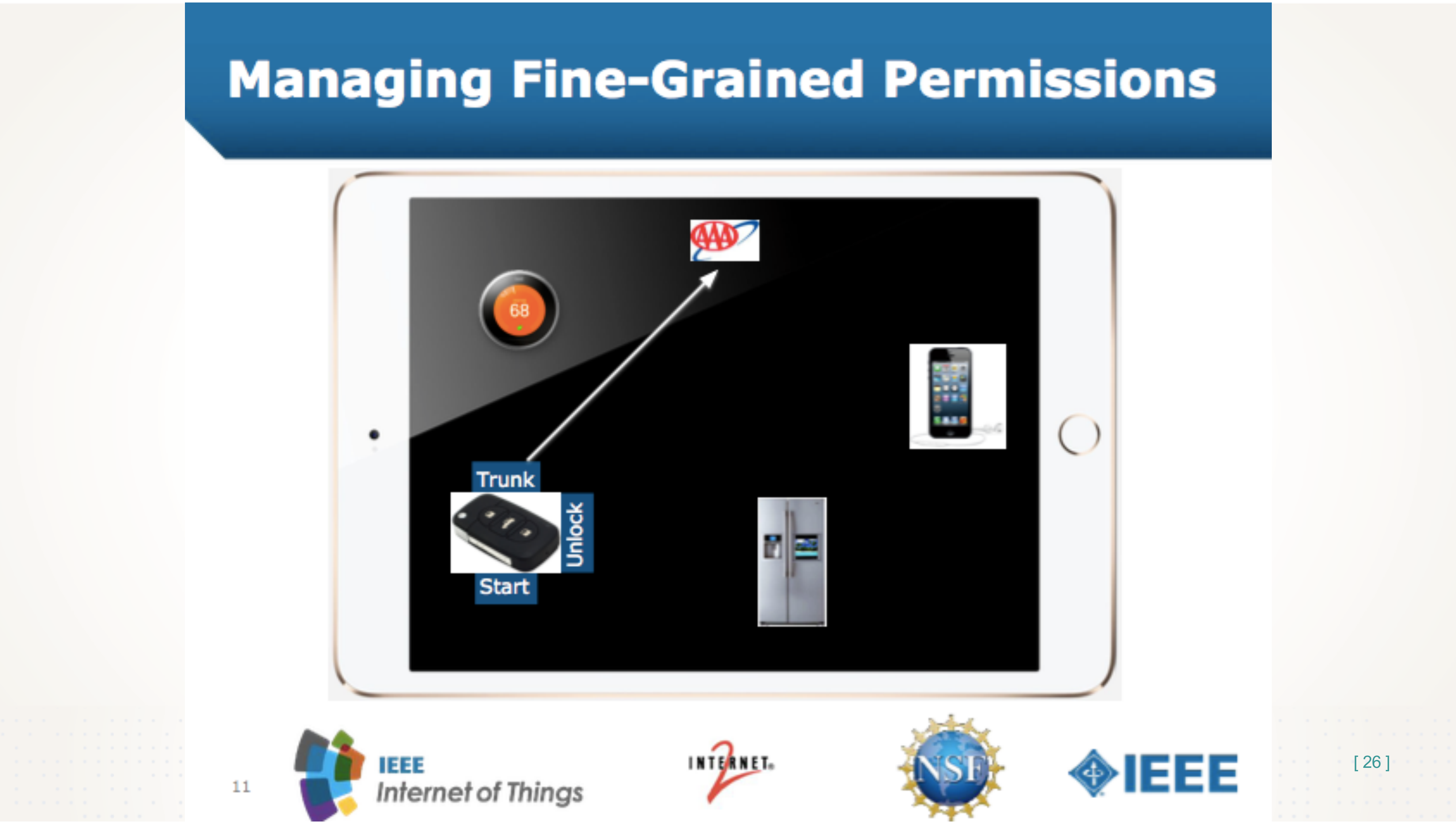
Managing Fine-Grained Permissions

IEEE Internet of Things

INTERNET2

NSF

IEEE



Managing Fine-Grained Permissions

Managing Fine-Grained Permissions

12

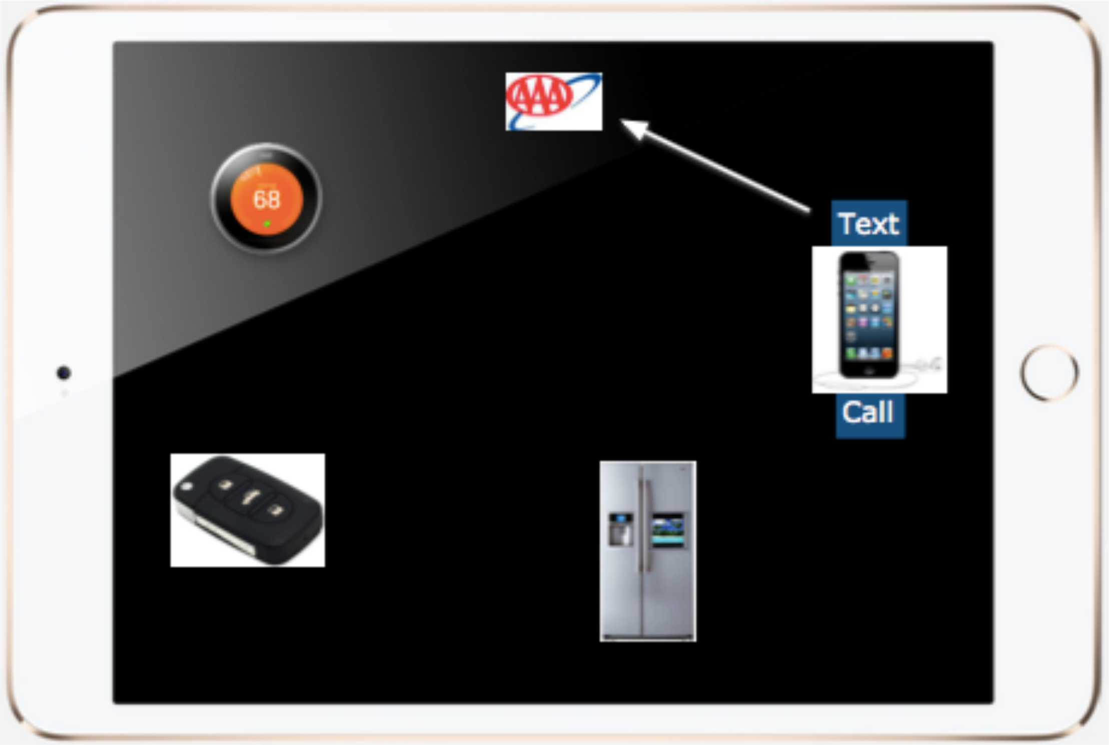
IEEE Internet of Things

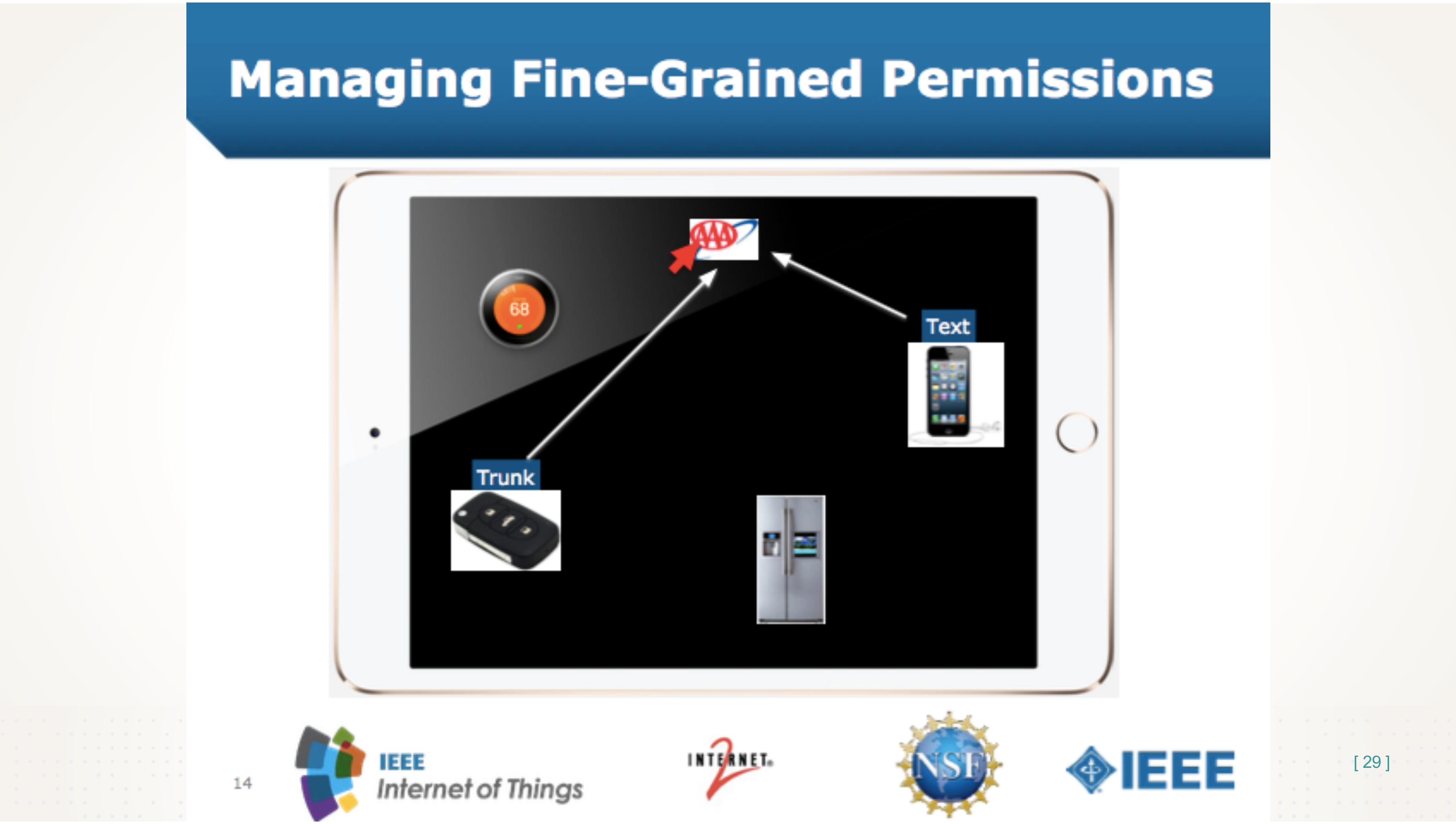
INTERNET2

NSF

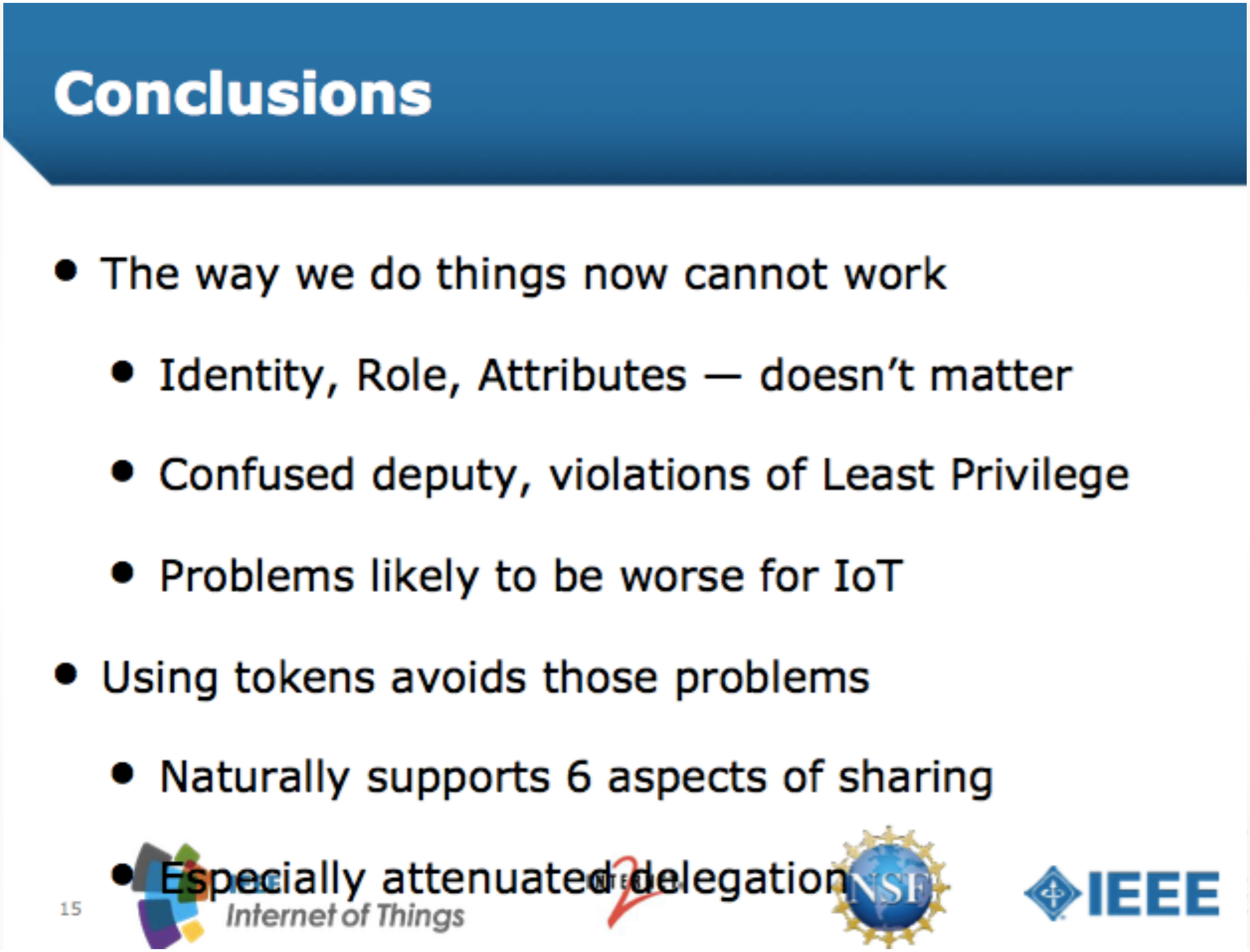
IEEE

Managing Fine-Grained Permissions





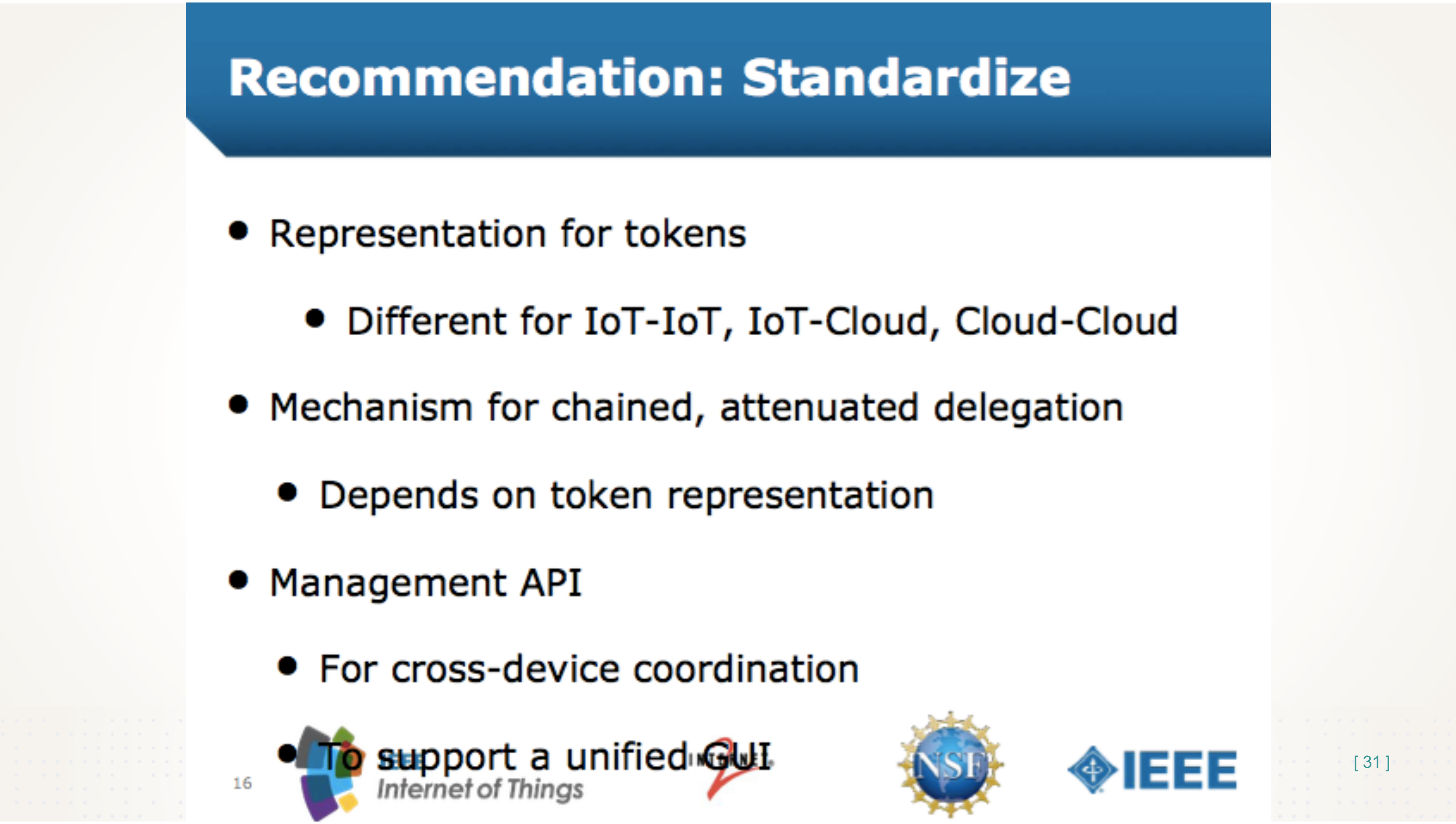
Managing Fine-Grained Permissions



Conclusions

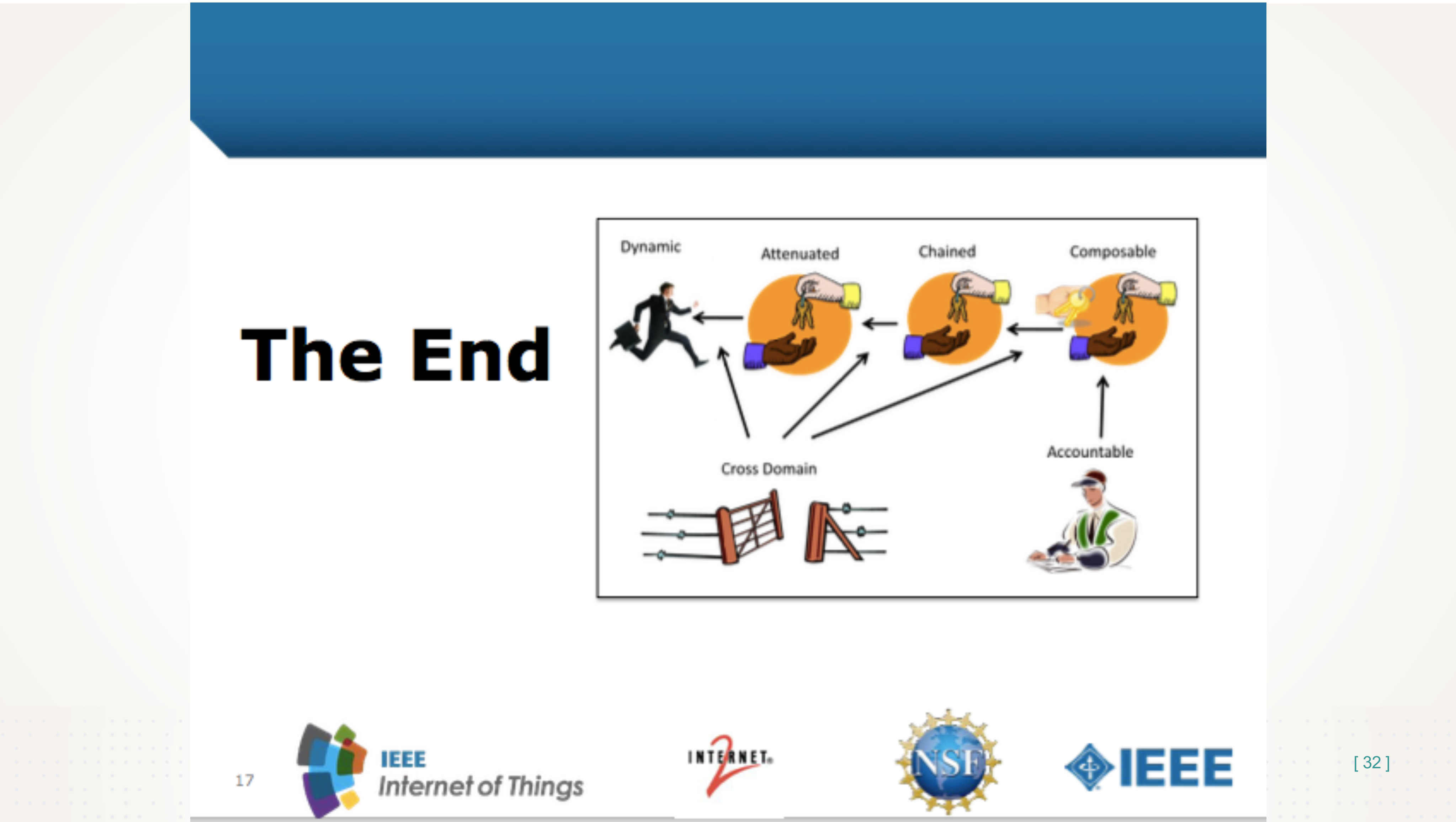
- The way we do things now cannot work
  - Identity, Role, Attributes — doesn’t matter
  - Confused deputy, violations of Least Privilege
  - Problems likely to be worse for IoT
- Using tokens avoids those problems
  - Naturally supports 6 aspects of sharing
  - Especially attenuated delegation

Internet of Things
NSF
IEEE



Recommendation: Standardize

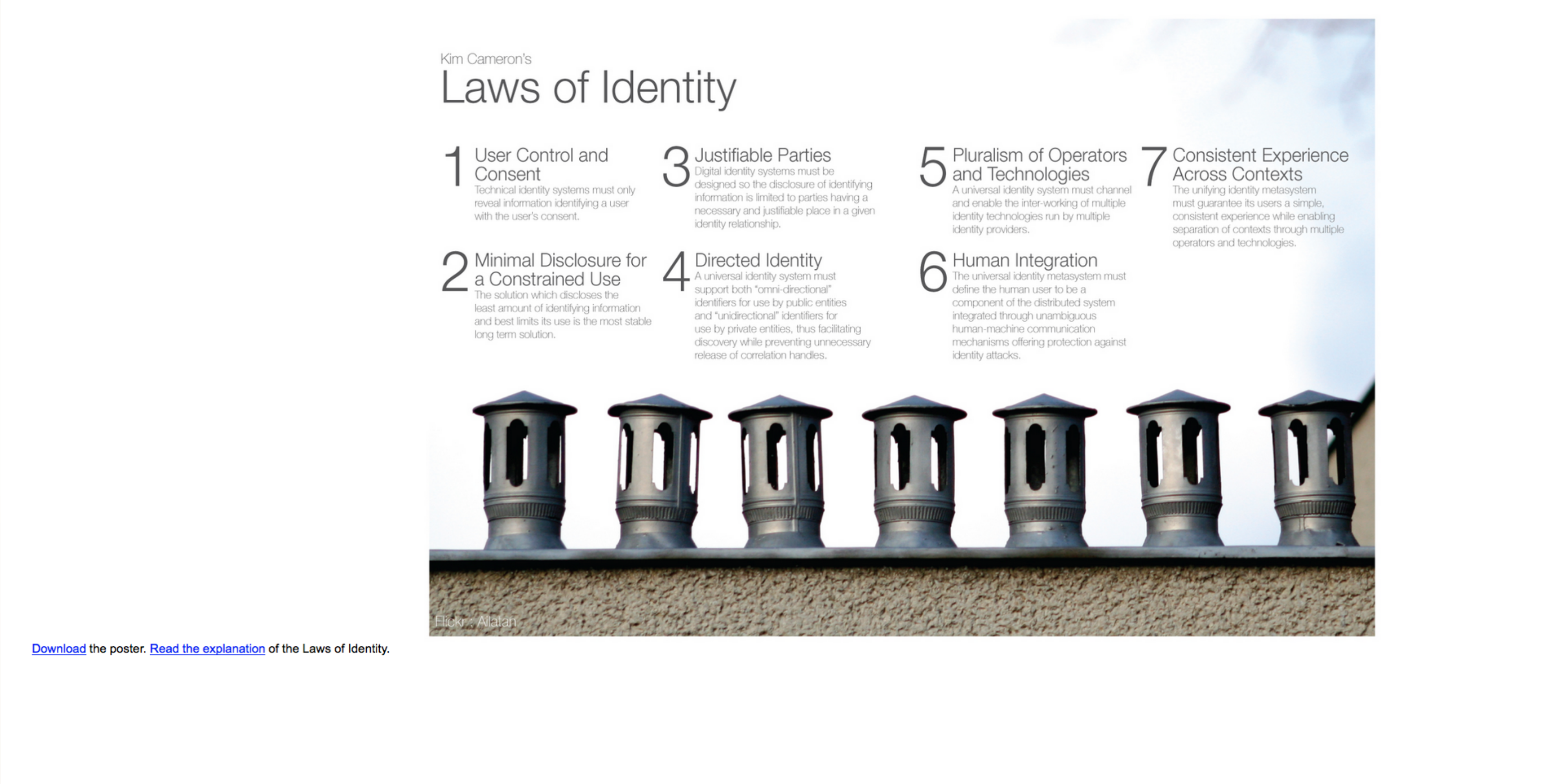
- Representation for tokens
  - Different for IoT-IoT, IoT-Cloud, Cloud-Cloud
- Mechanism for chained, attenuated delegation
  - Depends on token representation
- Management API
  - For cross-device coordination
  - To support a unified GUI



The End

Dynamic
Attenuated
Chained
Composable
Cross Domain
Accountable
IEEE
Internet of Things
INTERNET2
NSF
IEEE

Kim Cameron’s Laws of Identity



Kim Cameron’s

Laws of Identity

1 **User Control and Consent**
Technical identity systems must only reveal information identifying a user with the user’s consent.

2 **Minimal Disclosure for a Constrained Use**
The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

3 **Justifiable Parties**
Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4 **Directed Identity**
A universal identity system must support both “omni-directional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5 **Pluralism of Operators and Technologies**
A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6 **Human Integration**
The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7 **Consistent Experience Across Contexts**
The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Download the poster. Read the explanation of the Laws of Identity.

End to end trust

- At the network layer, end to end means traversing multiple hops in a coherent manner
  - Routing, diagnostics, QoS, reliability, security, congestion control, etc
  - Corresponding set of issues include signaling, performance, buffering, queueing, etc.
- At the identity layer, end to end trust means direct interactions between an identity provider (and the user) and the relying party, perhaps with federation mediation
  - Identifiers, schema, levels of assurance, SAML/OIDC protocols, attribute release and consent, metadata
  - Corresponding set of issues include discovery, privacy, man-in-the-middle attacks, consistent business practices, regulation, etc
- For IoT, end to end trust is all of above
  - All the standard network layer considerations
  - Many of the identity layer considerations
  - And more

Lessons from the middleware layer

- Interoperability: general standards and specific profiles per vertical/app/device/etc
- Be conservative in what you send and liberal in what you receive
- “There is no problem in Computer Science that can’t be solved with another level of indirection”
  - Except complexity
- Identifiers are the keys to discovery, privacy, etc
- Recommendations on boiling an ocean:
  - Small pieces, loosely coupled
  - Dealing with a marketplace and horses out of the barn
  - The importance of metadata

Panel Discussion

Where do we go next? How do we make TIPPSS real?

- Knowledgeable knowledge transfer
- Importance of middleware
- Medical centers
- Pilot use cases within the community

Recommended Next Steps

E2ET&S for IoT Recommended Next Steps

- **IoT exploration and collaboration**
  - For Research and Education: IT, researchers, lecturers, students
  - Collaborate with “The Things Network”
- **Smart Campus**
  - Increase awareness of IoT risk on campus
    - Shodan, Censys.io
  - Manage IoT systems and IoT vendors on campus
    - Leverage IoT vendor requirements document and process
    - Partner cross-organization and campus: IT, Facilities, Public Safety, Procurement
    - Inventory existing IoT devices: segment fixed vs mobile IoT devices
    - Develop guidelines on detecting, integrating, managing, and decommissioning fixed, mobile IoT devices
    - Develop infrastructure plan to support community owned IoT devices
- **In person Smart Campus meeting at Microsoft Workshop, February 2017**
- **Your ideas and discussion**

INTERNET2®

2016 TECHNOLOGY exchange

MIAMI FL SEPTEMBER 25–28

COLLABORATIVE INNOVATION COMMUNITY MEETING PART II: END-TO-END TRUST & SECURITY FOR IOT AND TIPPSS