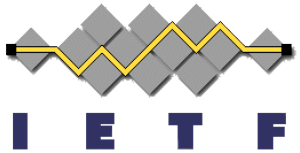
Smart Objects and the Internet Architecture

Fred Baker



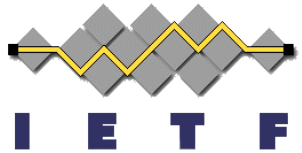
RFC 6272

- I wrote, with a lot of help, a document describing the RFCs we write and use as a toolbox from which one can build products
  - This was requested by US NIST for the purposes of the Smart Grid
- If I don't say so myself, it's recommended reading

"...the Network should enable an application in a particular domain to communicate with an application in any other domain in the information network, with proper management control over who and where applications can be interconnected."

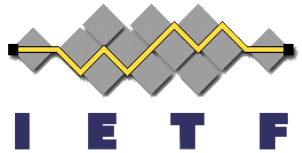
NIST Roadmap, Version 1.0, September 2009

We have some real challenges out there



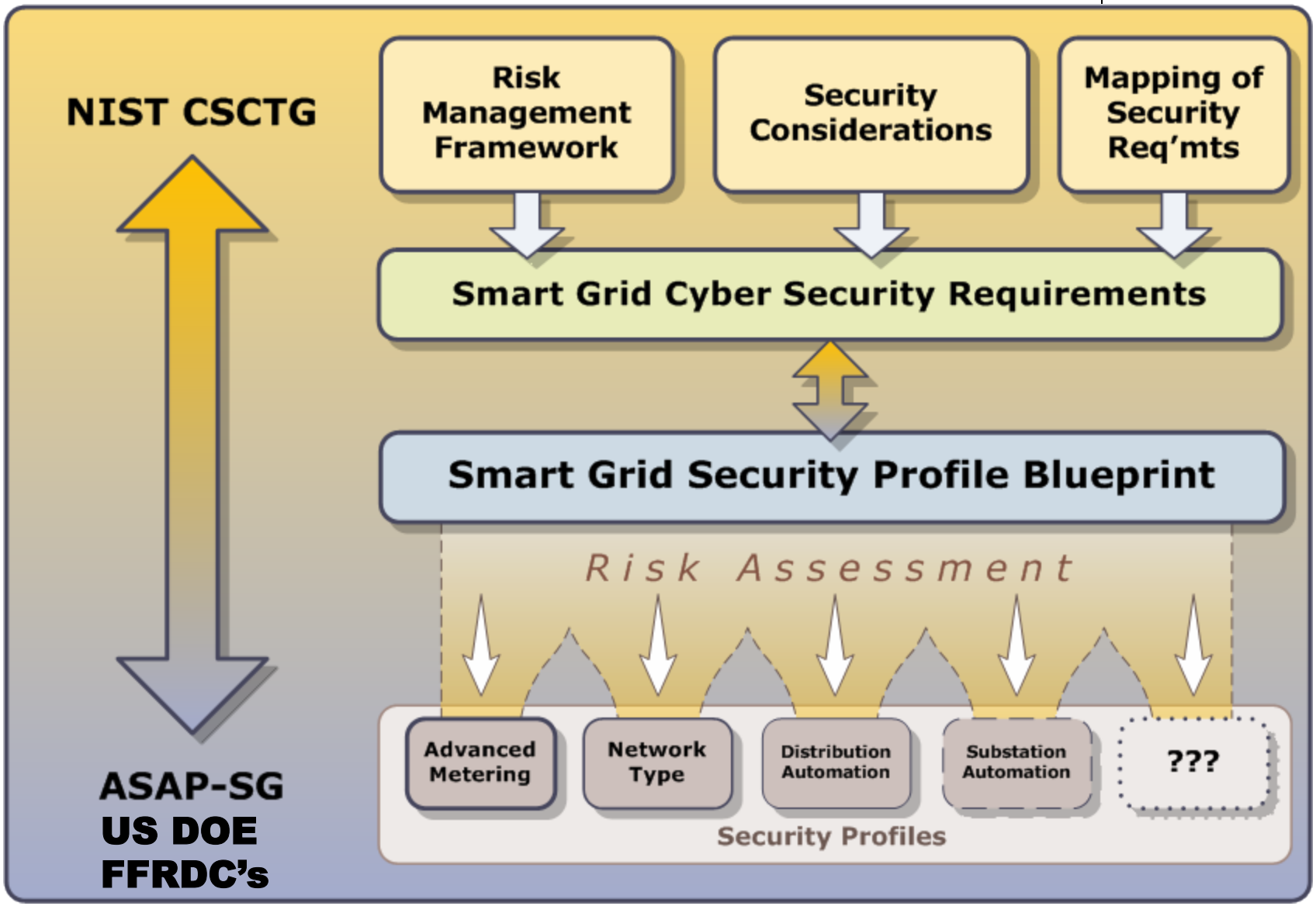
- Picking one…
  - Car companies tell us they want to burn a 128 bit address into an automotive appliance and use it to talk with the car's "mother ship"
    - Services similar to OnStar
    - Automotive maintenance reports
  - No comprehension that the IP Address presumes an Internet Architecture in which the prefix is a *locator*, and has to be scalably routable by the ISP
  - No comprehension that an IP datagram is routed from and to a *customer*…
- A better alternative: an architecture for trusted communications
  - Whatever *address* I am using, I identify myself to my peer using protocol exchanges such as HIP/ESP or D/TLS

Don’t misunderstand the intent of networks of Smart Objects



- *They don’t all intend to use the Internet as we understand it*
  - *Smart Grid, specifically, likely to be a parallel network for the most part*
- They do plan to use IP and some of the related protocols
  - If a protocol doesn’t meet their needs, they plan to change or replace it
  - Health care likely a VPN, IPsec Transport Mode, https, or D/TLS-based

DOE / NIST / UCAIug / ASAP-SG Security Effort



What kinds of security mechanisms?

Communication Layer	Type of control	Example
Data Content	End to end integrity in message-based exchange	W3C XML Signature
Application Layer	Application to application authentication, authorization, encryption	TLS, HTTPS, DKIM, S/MIME, SSH
Network Layer	System-to-system authentication, authorization, encryption	IPsec ESP
Physical/Link Layer	Limited Membership	SSID, IEEE 802.1X with EAP-TLS