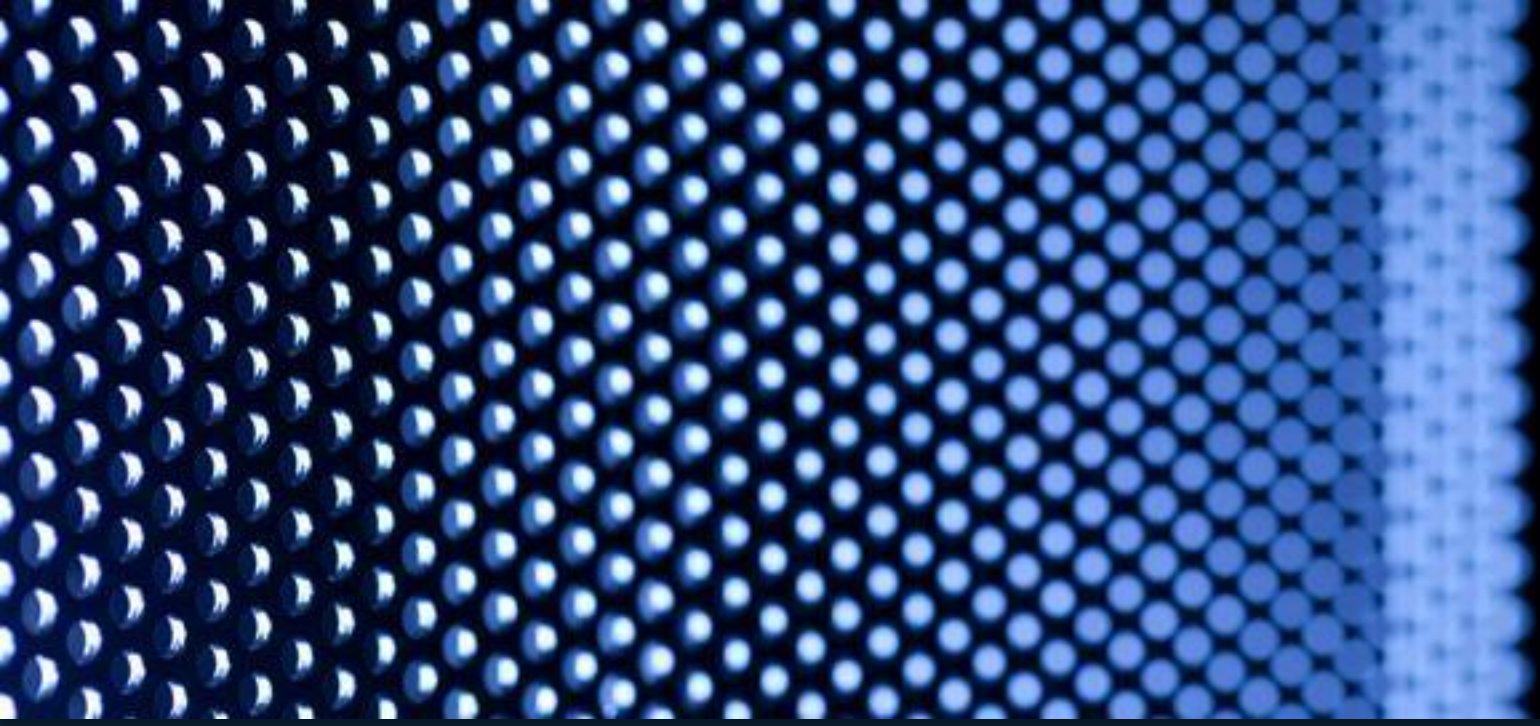


VERISIGN

Living in a World of Decentralized Data

Dr. Burt Kaliski, Jr.
Senior Vice President and CTO, Verisign

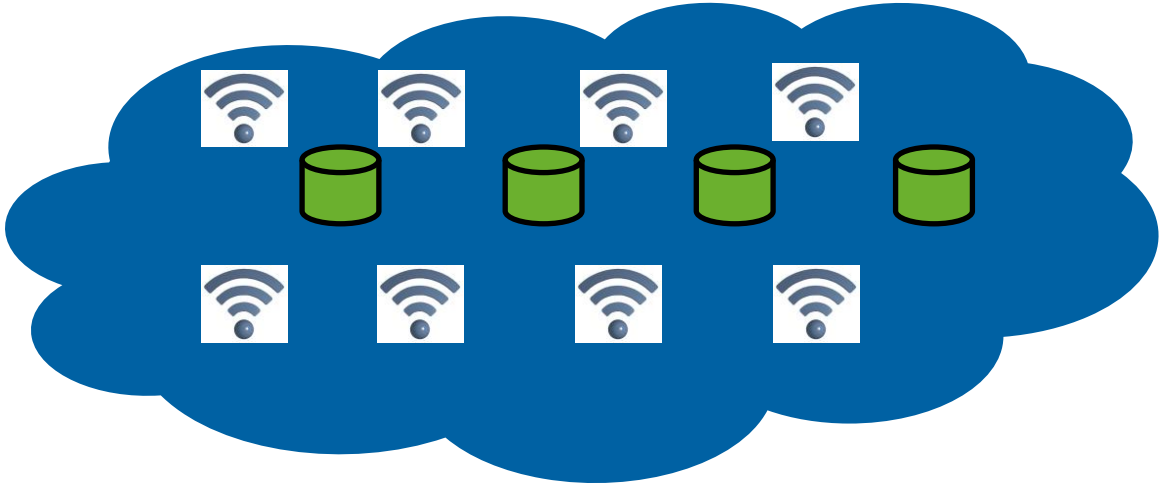
NDSS Workshop on Security of Emerging Networking Technologies (SENT)
February 8, 2015

Abstract

- Emerging networking technologies such as the Internet of Things present unique challenges due to the significant decentralization of both data generation and data distribution.
- Living in this world of decentralized data may require new answers to traditional questions about security, ranging from what to authenticate, to how to bootstrap trust, to how to share threat indicators.
- This interactive talk will facilitate a discussion of the possible answers, drawing examples from related research at Verisign on the Domain Name System.

Agenda: Security in an Emerging World

Emerging Networking Technologies
=
Cloud of **Data-Generating Devices** and
Data Distribution Points



- How do applications operate securely in this world?
- 10 interactive questions with examples from Verisign's research on Domain Name System (DNS)

1. Data, Device, or Distribution Point?

Q. Do you authenticate the data, the device, or the distribution point?

A. Depends what you're interested in …

DNS records vs. name servers vs. intermediaries

2. Authentication Methods

Q. How do you authenticate the data, the device, or the distribution point?

A. Digital signatures?
Symmetric authentication?

2. Authentication Methods – cont'd

Q. More generally, how do you encrypt data, exchanges with devices, distribution points?

A. DTLS? Something else?

DNSSEC signatures, DPRIVE working group

3. Public Key Distribution

Q. How do you get the public key for verifying the digital signature?

A. Certificates? Key servers?

3. Public Key Distribution – cont'd

Q. How do you get the certificate authority's public key?

A. Trust list?

3. Public Key Distribution – cont'd

Q. How do you know the certificate is still valid? What if it's revoked?

A. Status checks? Revocation lists? Short validity periods?

3. Public Key Distribution – cont'd

Q. How do you know this is the *correct* certificate authority?

A. ??

DANE TLSA record for publishing certificates

4. Application Authentication

Q. How does the device or data distribution point authenticate you?

A. Digital signatures?
Symmetric authentication?
Third-party models?
Passwords? Multi-factor?

Passwords, multi-factor for registration operations via Extensible Provisioning Protocol (EPP)

5. Trust Relationships

Q. How does the device "bootstrap" its trust relationships?

A. Root keys? Trust lists? Management keys? Pairing?

DNSSEC root keys

6. Cryptographic Algorithms

Q. Which cryptographic algorithms do you use?

A. Public-key – RSA, ECC, other? Symmetric key? Hash functions? Group signatures, other advanced constructions?

Many of these, plus research into Merkle tree signatures for long-term ("post-quantum") security

7. Denial-of-Service (DoS) Attacks

Q. How do you protect the device or data distribution point from DoS and other attacks?

A. Cloud proxy? Network traffic management? White lists?

All of the above and more …

8. Threat Indicators

Q. How do devices and data distribution points share indicators of potential threats?

A. ??

… especially challenging in a *decentralized* world

8. Threat Indicators – cont'd

Q. Whom do they share indicators with?

A. ??

DDoS cloud signaling protocol
`draft-teague-open-threat-signaling-00`, January 2015

9. Security and Stability

Q. How do you measure the security and stability of an overall system?

A. ??

Root zone monitoring – RSSAC-001 and -002; DNS-OARC studies

10. Names

Q. How do you name things?

A. Global names? Local names? Device identifiers? Hashes of keys? Information-centric networking?

DNS names (of course) – and other identifiers (e.g., email addresses) encoded as DNS names

Summary: Questions for the Emerging World

1. Data, Device or Distribution Point
2. Authentication Methods
3. Public Key Distribution
4. Application Authentication
5. Trust Relationships
6. Cryptographic Algorithms
7. Denial-of-Service Attacks
8. Threat Indicators
9. Security and Stability
10. Names

powered by

VERISIGN™