Engineering, Operations & Technology
Boeing Research & Technology

Delay / Disruption Tolerant Networking (DTN) Security Key Management

Fred L. Templin
fred.l.templin@boeing.com

Background

- **The Internet Protocols (TCP/IP) are ubiquitous:**
  - Most widely-deployed networking protocol suite in human history
  - Backbone for all data communications in the global Internet
  - Support wide diversity of applications (e.g., e-mail, file transfer, web browsing, social media, Internet telephony, streaming video, etc., etc.)
  - Connect billions of users worldwide
- **Best suited to "well behaved" paths:**
  - Low to moderate end-to-end delays (usec/msec/sec), packet loss, reordering, per-packet queuing delays in network middleboxes
  - "Conversational" data exchanges
  - Client/server architectures
  - Reactive congestion control
  - End-to-end flow control and retransmission
  - Data transmission order implicit in data arrival order – no need for explicit ordering markings

Delay/Disruption Tolerant Networking (DTN)

- **New Requirements That Don’t Fit the Mold:**
  - Moderate to long end-to-end delays (minutes/hours/days)
  - Moderate to high end-to-end packet loss (i.e., significant disruption)
  - Moderate to high queuing delays (store, carry, forward)
  - “Open Loop” data exchanges (bulk data transfers, public service bulletins, remote command and control messaging, situation awareness dissemination on scheduled/opportunistic contacts, etc.)
- **Use Cases Not Always Satisfied by TCP/IP:**
  - Space-based Communications (ISS, deep-space, etc.)
  - Satellite-Assisted Communications for Isolated Ground Systems
  - Civil Aviation (loss of comms; bulk transfers, etc.)
  - Unmanned Aerial Systems (UAS) operating in remote regions
  - Many others

➤**DTN provides a practical solution**

DTN for Space Systems Communications

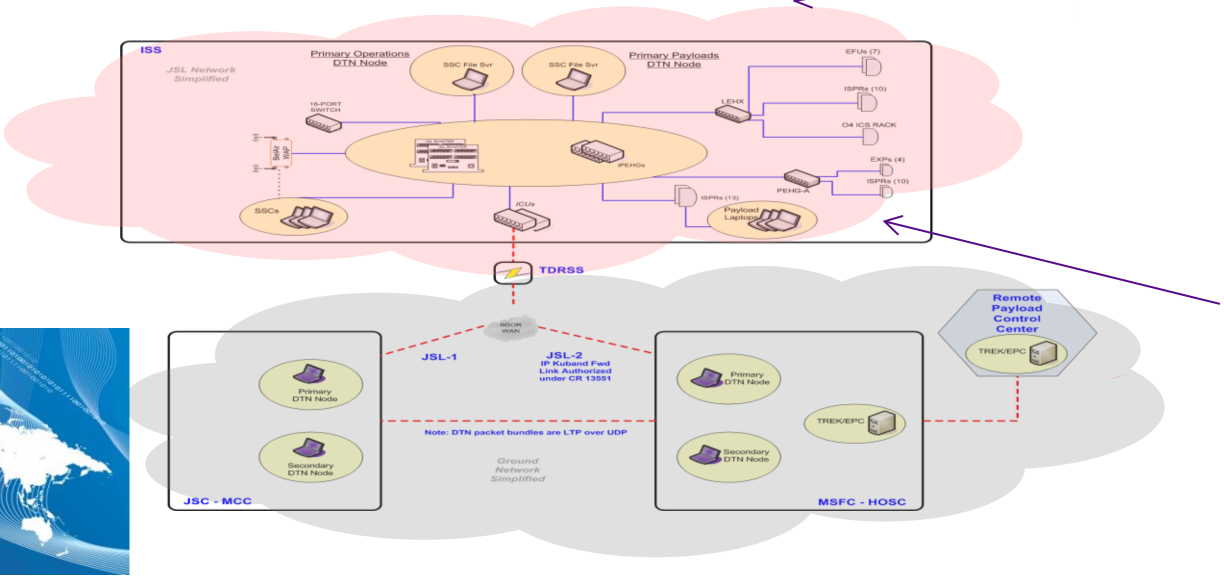
- **DTN Replaces Customized (non-standard) Communications Between International Space Station (ISS); Ground Systems**
  - DTN overcomes limitations of RF space links
    - Tracking and Data Relay Satellite (TDRS) Availability Issue (~30% outage)
    - Communications Latency in Ground/TDRSS/ISS RF Links
- **DTN Compatible with Deep Space Communications**
    - One-Way Light Time (OWLT) from Earth to Mars ~4min minimum
    - Satellite Assist Not Always Available – long outages
- **DTN Provides Space System Support for Isolated Ground Systems**
    - Data Exchanges Only Possible During Satellite Over-Flights
- **DTN Needs Well-Architected Security Solutions**
  - Current security based on piecemeal solutions; local security schemes
    - Delay/Disruption-Tolerant Security Standards Needed

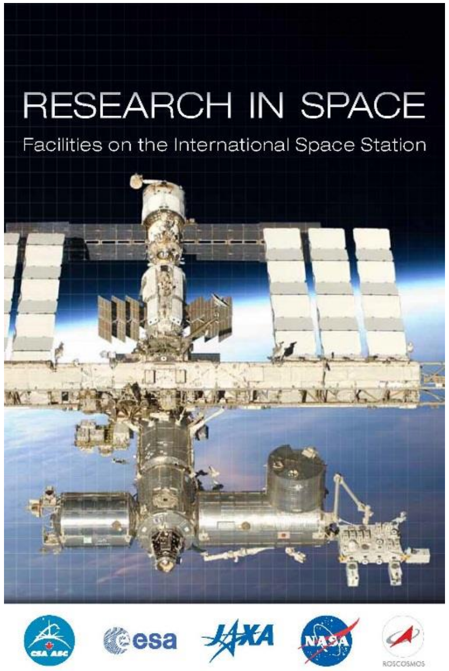
The InterPanetary Networking Special Interest Group (IPNSIG) is moving forward to an Internet that's Interplanetary in scope and function… (http://ipnsig.org)

Source: NASA

DTN for International Space Station (ISS)

- **ISS is an Internet unto itself**
  - On-board networked devices connected as a private Internet
    - ➢Separate from the Earth-based Internet
    - ➢Separate routing and addressing domain
  - Well-connected on-board devices (low delay/disruption)
  - Communications with off-board control stations subject to TDRSS availability
- **DTN Security Solutions Needed to Secure On-board Devices**
    - ➢Need: DTN Security Key Management




RESEARCH IN SPACE

Facilities on the International Space Station

DTN Security Key Management Requirements

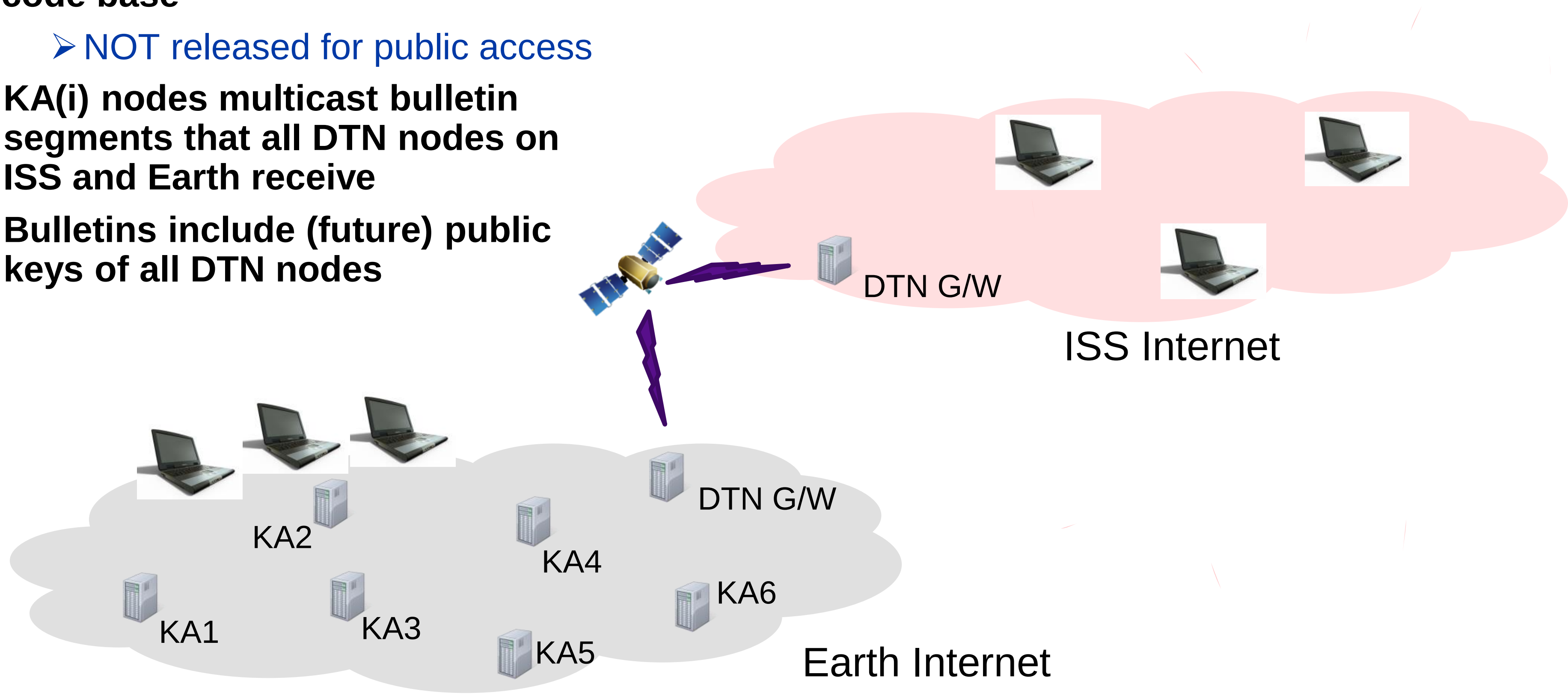
- **MUST NOT Rely on Online Access to a Public Key Infrastructure (PKI)**
  - Low-delay online access using standard TCP/IP connections may never be available
  - Even if the key is retrieved using some delay-tolerant pull request, the opportunity to decrypt the data may be gone by the time the key arrives
    - Traditional PKI incompatible with DTN
- **MUST Ensure that Security Keys are Put in Place Before they are Actually Needed**
  - If a source encrypts or signs a bundle of data using its private key, each DTN node in the path must have access to the public key **before** the bundle arrives
    - Otherwise, the bundle would be rejected due to security policy
- **MUST be Based on Trust Anchors Common to All DTN Nodes**
  - Needed to ensure that all DTN nodes will receive public keys from a secured key authority
    - DTN nodes cannot simply accept public keys directly from each other
    - Otherwise, the network and all devices that use it are inherently compromised
- **MUST be Based on a Publish/Subscribe Model**
  - On-demand retrieval from a traditional server not delay tolerant
  - Requires one or more Key Authorities (KAs) to publish **Bulletins** to which all DTN nodes subscribe
    - Bulletins must reach all DTN nodes in the network over the same long-delay links that would carry ordinary data packets
    - Bulletins therefore must publish keys to be used AT SOME TIME IN THE FUTURE

DTN Security Key Management Requirements (Cont’d)

- **MUST NOT Introduce a Single Point of Failure**
  - All DTN nodes cannot simply accept a monolithic bulletin from a singe KA node
    - ➢ What if the KA node fails?
    - ➢ What if the KA node is hacked?
    - ➢ What if the KA node begins sending erroneous data?
- **MUST Distribute the Key Distribution Service to multiple KAs**
  - KAs agree on a bulletin through control message exchanges
    - – not delay tolerant, but doesn’t need to be
  - Each KA publishes a few **overlapping pieces** of the bulletin
  - Each DTN node receives the pieces and reassembles them into a complete bulletin
    - ➢ It is OK if one or more of the KAs fails, because the pieces are overlapping and DTN nodes will be able to reconstruct the full bulletin
    - ➢ It is OK if one or more of the KAs has been hacked, because the integrity of the bulletin will be asserted by the consensus agreement of all KAs
    - ➢ It is NOT OK if all KAs fail or become compromised; at least a few non-compromised trust anchors must be present
  - **MUST Assure that the Key Distribution Service is Highly Available and Hardened Against Compromise**
    - ➢ **No Different than core Internet svc’s such as the Domain Name System (DNS)**

Delay Tolerant Key Administration (DTKA)

- **Original idea from NASA JPL (Scott Burleigh)**
- **Based on distributed KA nodes that provide bulletin services to DTN clients**
- **Prototype implementation in Interplanetary Overlay Network (ION) code base**
  - NOT released for public access
- **KA(i) nodes multicast bulletin segments that all DTN nodes on ISS and Earth receive**
- **Bulletins include (future) public keys of all DTN nodes**



DTKA Technical Background

- **Security model for DTN is based on ephemeral session keys**
  - Assumes that security keys are ephemeral, that is, each DTN bundle carries a one-time use key rather than a persistent session key
  - Use DTKA private/public key to encrypt/decrypt ephemeral key
  - Use ephemeral key to decrypt / authenticate data
- **DTKA organized as a group of N Key Authority (KA) nodes**
  - Each KA node has all current public key information for the network
- **EACH DTN node generates its own public/private keys and sends these to each KA node**
- **DTKA issues key assertions and revocations in bulletins sent to all DTN nodes**
  - Each KA node sends only a subset of blocks of the entire bulletin
  - Each block is erasure-coded for FEC in case some blocks are lost , corrupted, or deemed untrustworthy
  - Parity blocks for error detection
  - Receivers reassemble the bulletin from union of blocks received

DTKA Technical Background (cont’d)

- **DTN nodes use keys they have received in bulletins based on bundle creation times**
  - Keep track of recently received public keys for each node
  - Use the newest key that is no younger than the bundle creation time
- **Since multiple keys are kept with creation times, no need to synchronize transmission and reception key selection**
- **Nothing in the key distribution system is secret – it’s all public information**
  - Security based on DTN node’s trust relationship with KAs
- **Result**
  - All public keys distributed securely
  - Key management is automated (with human intervention for revocation)
  - No multi-message exchanges over long-delay links
  - Ephemeral keys instead of session keys
  - No single point of failure or compromise

DTKA Practical Deployment Considerations

- **Scalable, Reliable Multicast**
  - DTN Bundle Protocol (BP) reliably delivers bundles to one or more recipients
  - Reliability based on convergence layer protocols such as TCP, LTP
  - Reliable delivery is “hop-by-hop”
    - Each hop needs to take custody from the previous hop to ensure that end-to-end delivery is reliable
  - Multicast reliable delivery also based on hop-by-hop convergence layers
    - But, large-scale reliable multicast is an end-to-end consideration
- **Security of Key Authority Servers is a Fundamental Requirement**
  - Just as for core Internet services (e.g., the DNS), the DTN Key Authority service must be protected against network-based and physical security attacks
  - System is resilient to one or more elements being compromised, but bringing down all nodes essentially brings down the DTN
  - History has proven that services of this nature in the public Internet can be protected against comprehensive destruction
    - MUST ensure network and physical security to protect DTKA

DTKA Practical Deployment Considerations (cont'd)

- **Dealing with Nodes (Re)Entering the DTN After a Long Time Away**
  - Sometimes DTN nodes can go offline for extended periods of time (days/weeks/months) – same consideration as for a new DTN node entering service for the first time
  - Upon (re)entering the DTN, the node has to publish its public key via the KAs
  - This "first contact" trust establishment is crucial to the security of the entire system – need to have a way for the new DTN node to trust the KAs, and for the KAs to validate the identity of the DTN node
- **DTKA in mobile networks**
  - Ground stations talking to ISS are not a problem, since the DTN topology does not change
  - Mobile ad-hoc networks typically show up in unmanned aerial vehicle (UAV) networks, tactical military networks, etc.
  - In that case, portions of the DTN may become detached from the rest of the DTN and re-attach at a different point of the DTN at a later time.
  - This is more of a routing issue than a DTKA issue, but routing aspects of DTKA need to be understood
- **DTKA for the ISS**
  - Continue working with Boeing BDS and NASA partners to understand the operational limitations of the environment
  - Determine a best layout of DTKA critical infrastructure
  - Harmonize administrative control of critical infrastructure with ISS policies and practices

Summary

- **The International Space Station (ISS) is an Internet unto itself**
  - Connects to the ground control network via DTN gateways that can support operation even across long delays or disruptions
  - Needs to have access to public keys of all potential correspondents
- **Traditional PKI Services are not Delay Tolerant and not Candidates for Operation in DTNs**
  - Need a publish/subscribe model to publish keys that will enter use at some point in the future
  - Works across long delay/disruption paths
  - Works when not all nodes are in the same Internet, since DTN joins Internets together
- **DTKA is the Core Engine for Publication of Public Key Bulletins**
  - Like any other critical infrastructure for major data communications networks (such as the public Internet), security requires a fundamental trust basis as a foundation
  - For DTKA, the KAs are the trust anchors and must be well managed and secured
  - Once the DTKA critical infrastructure is secured, public key security for DTN nodes naturally follows
- **Practical Deployment Considerations for DTKA Subject for Ongoing work**

  ➢ **Goal: Adapt a DTKA-like Approach to Secure the ISS**

Backups

Engineering, Operations & Technology | **Boeing Research & Technology**