Forward Secrecy in ICN?

A) Yes

B) No

C) It Depends…

What is Forward Secrecy (FS)?

Definition: exposure of principals' long-term secret keys does not compromise the secrecy of previous session keys.

Attacker: Someone (or something) logging traffic and trying to recover long-term keys.

Good and Bad

Benefits:

- Minimal data and key compromise windows
- Reduced attack vector

Drawbacks:

- Requires protocols, techniques, etc. for deriving fresh or updating keys regularly

ICN Literature (Subset) Breakdown

Work	Not FS
Yu, Yingdi, Alexander Afanasyev, and Lixia Zhang. "Name-Based Access Control." Named Data Networking Project, Technical Report NDN-0034(2015).	✗
J. Kurihara, E. Uzun and C. Wood. An encryption-based access control framework for content-centric networking. In IFIP Networking Conference (IFIP Networking), pages 1–9. IEEE, 2015.	✗
T. Chen, K. Lei, and K. Xu. An encryption and probability based access control model for named data networking. In IEEE International Performance Computing and Communications Conference (IPCCC), pages 1–8, 2014.	✗
S. Misra, R. Tourani, and N. Majd. Secure content delivery in information-centric networks: design, implementation, and analyses. In Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking, pages 73–78, 2013.	✗
R. S. da Silva and S. Zorzo. An access control mechanism to ensure privacy in named data networking using attribute-based encryption with immediate revocation of privileges. In 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), pages 128–133, 2015.	✗
B. Hamdane and S. G. Fatmi. A credential and encryption based access control solution for named data networking. In IFIP/IEEE International Symposium on Integrated Network Management (IM), pages 1234–1237, 2015	✗
M. Ion, J. Zhang, and E. M. Schooler. Toward content-centric privacy in icn: attribute-based encryption and routing. 43(4):513–514, 2013.	✗
B. Li, A. Verleker, D. Huang, Z. Wang, and Y. Zhu. Attribute-based access control for icn naming scheme. In IEEE Conference on Communications and Network Security (CNS), pages 391–399, 2014.	✗
C. Ghali, M. Schlosberg, G. Tsudik and C. Wood, "Interest-Based Access Control for Content Centric Networks," ACM Conference on Information-Centric Networking (ICN), 2015.	✗
C. Wood, E. Uzun, et al. Flexible end-to-end content security in ccn. In IEEE 11th Consumer Communications and Networking Conference (CCNC), pages 858–865, 2014.	✗
S. Singh. A trust based approach for secure access control in information centric network. International Journal of Information and Network Security (IJINS), 1(2):97–104, 2012.	✗
N. Fotiou, G. Marias, and G. Polyzos. Access control enforcement delegation for information-centric networking architectures. In Proceedings of the second edition of the ICN workshop on Information-centric networking, pages 85–90. ACM, 2012	✗

ICN Literature Summary

Existing “object encryption” techniques are not forward-secure

What's in the "Real World"?

- Application layer
  - DNS-over-TLS
  - HTTPS
- Session-layer
  - TLS
  - DTLS
  - QUIC
- Transport-layer
  - tcpcrypt

What's in the "Real World"?

- Application layer
  - DNS-over-TLS FS
  - HTTPS FS
- Session-layer
  - TLS FS
  - DTLS FS
  - QUIC FS
- Transport-layer
  - tcpcrypt FS

Claims

- If ICN is to be used for “Internet or IoT applications,” then it should at least be at parity with current Internet protocols
  - What else will it be used for?...
- Current Internet protocols are forward secure **because** key management is difficult
  - Key compromise should not harm past communications (=data transfers)

Argument #1: Data at Rest vs. Data in Transit

Transferring encrypted data at rest

Transferring (encrypted) data encrypted in transit

Argument #1: Data at Rest vs. Data in Transit

Transferring encrypted data at rest

$\neq$

Transferring (encrypted) data encrypted in transit

- Data in transit can be captured
- Data at rest is more difficult to acquire
- In both cases, the keys protecting the content are protected **the same way**
- Ergo, transporting data without forward secrecy is distinctly less secure

Argument #2: Untrusted Caches are Not Helpful

Untrusted caches:

- Enable data correlation across multiple users
- Perform **no** authorization checks for interests
- Swallow usage statistics and make per-content accounting difficult

Argument #3: Network Names Reveal too Much

- TLS-protected traffic reveals IP addresses and ports
- Unencrypted and partially-encrypted interest names reveal all or some data context

```
/netflix/content/media/movies/TheAvengers/Chunk=0
/akamai/cdn/0x1827347182331…
```

- The name encryption “boundary” in ICN is an application decision…
  - … and developers make mistakes.

Q1) Under what conditions does transport security require forward secrecy?

Q2) Can object encryption subsume transport security?

Q3) Forward Secrecy in ICN?

A) Yes

B) No

C) It Depends…