“**Opportunistic**” Encryption

Strengthening the Internet Against Pervasive Monitoring (STRINT)

- 07: “Trust Issues with Opportunistic Encryption”
- 12: “Opportunistic Encryption for HTTP URIs”
- 27: “Is Opportunistic Encryption the Best Answer? Practical Benefits and Disadvantages”
- 32: “Simple Opportunistic Encryption”
- 40: “Levels of Opportunistic Privacy Protection for Messaging-Oriented Architectures”
- 66: “Opportunistic Keying as a Countermeasure to Pervasive Monitoring”
- 46: “Replacing Passwords on the Internet AKA post-Snowden Opportunistic Encryption”

- 07: “Trust Issues with Opportunistic Encryption”
- ~~12: “Opportunistic Encryption for HTTP URIs”~~
- 27: “Is Opportunistic Encryption the Best Answer? Practical Benefits and Disadvantages”
- 32: “Simple Opportunistic Encryption”
- 40: “Levels of Opportunistic Privacy Protection for Messaging-Oriented Architectures”
- 66: “Opportunistic Keying as a Countermeasure to Pervasive Monitoring”
- 46: “Replacing Passwords on the Internet AKA post-Snowden Opportunistic Encryption”

40: “Levels of Opportunistic Privacy Protection for Messaging-Oriented Architectures”

- Deep-dive on encryption for messaging
  - Channel vs. end-to-end
  - DNS for key discovery

66: “Opportunistic Keying as a Countermeasure to Pervasive Monitoring”

- Survey of “opportunistic” and related encryption in existing standards
  - e.g., IPsec, VOIP, IMAP/POP, SSH, TLS
- Attempts to collect relevant terminology
  - Opportunistic Encryption / Keying
  - Anonymous Encryption / Keying

07: “Trust Issues with Opportunistic Encryption”

27: “Is Opportunistic Encryption the Best Answer? Practical Benefits and Disadvantages”

- The heart of the matter - benefits and risks of unauthenticated encryption
  - “[E]nd users can develop a false sense of security.”
  - “[OE] may even cause as much harm as good.”
  - “[OE] can and should be used as a last resort to provide a minimal level of confidentiality to protect end users' privacy.”

32: “Simple Opportunistic Encryption”

- Argues that introducing encryption at the transport layer is lowest-impact
  - …but authentication is an application concern
- Proposes TCPCrypt as the way to do this
- With Password-Authenticated Key Exchange (PAKE)
  - Auth is app-specific

46: “Replacing Passwords on the Internet AKA post-Snowden Opportunistic Encryption”

- Build authentication on top of encrypted connections

- Secure password store

- PAKE

Related

- Some experimentation in HTTPbis with "**TLS for HTTP:// URIs**"
  - Authenticated vs. unauthenticated TBD
  - Confusion, encouraging active attacks and opportunity cost are main concerns
- "**Explicit proxy**" confusion exposed how even obvious differences in security properties can be misunderstood by an educated audience

- Discussion of more encryption in HTTP has highlighted reliance upon unencrypted access:
  - Captive portals
  - Virus scanning
  - Policy imposition
  - Optimisation
- TLS MITM is becoming more common

suggested discussion points

1. Terminology

- ~~Opportunistic Encryption~~
- Authenticated vs. Anonymous
- Fail-Safe vs. Fail-Silent (or “safe vs. silent”)

2. Ratholes to Avoid

- Specific technologies / solutions / layers (yet)
- Speculation on User Interface / eXperience (although it is incredibly important and a blocker for most approaches)

3. Questions

1. Is protecting against passive attacks worth the costs/risks?
    1. Confusing users and administrators with more complex, nuanced idea of “security”
    2. Encouraging (sometimes trivial) active attacks
2. Is the use of encryption without authentication appropriate? When?
3. Is failing encryption silently appropriate? When?
4. Are either appropriate for new protocols?
5. Are there alternate ways to overcome deployment issues of “full” encryption?
6. What other work does more ubiquitous encryption imply?