Steve Tate: Research Summary
What I do and why I do it

Edward Snowden: NSA whistleblower
Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.

Apple and the SSL/TLS bug: Open questions
Critical crypto bug leaves Linux, hundreds of apps open to eavesdropping
This GnuTLS bug is worse than the big Apple "goto fail" bug patched last week.

'Heartbleed' bug undoes Web encryption, reveals Yahoo passwords
A flaw in software that's widely used to secure Web communications means that passwords and other highly sensitive data could be exposed. Some say they've already found hundreds of Yahoo passwords.

Microsoft SSL bug could be worse than Heartbleed, say researchers

Scope of the problem:
OpenSSL consists of 460,413 lines of code!

Some current projects:
- Machine-checked proof of security for a fundamental encryption mode
- Machine-checked proof of correctness for OpenSSL “big number” routines
- Starting soon: “bug bounty” club focused on analysis of widely-used software