SaTC: CORE: Small: Usable Secure Email

Project Summary

This proposal addresses the long-standing problem of providing usable, secure email for the general public. A focus throughout the proposal is to understand issues that prevent users from adopting secure email and then designing for adoptability. This requires addressing user perception of risk, and the efficacy of software to mitigate risk, in addition to making usable software for public key cryptography. The goal is to provide tools that help users incorporate secure email into their daily habits.

Research tasks center on key management, including key discovery and authentication, key storage and portability, and forward secrecy. To conduct experiments on these research topics, the team will continue their development of a browser extension they have developed, called MessageGuard, that integrates secure email into existing webmail systems such as Gmail and Yahoo Mail. This system will enable the team to explore both adoptability and usability, since vast numbers of people use webmail on a daily basis. Evaluation of secure email systems will include both laboratory experiments to gather data on research prototypes and long-term studies to provide insight into how users integrate secure email into their everyday habits.

Intellectual Merit
Sending and receiving information securely online is a basic need in our connected world. However, one of the most frequently used online applications – email – remains largely insecure for all but the most expert users. The technology needed to deploy secure email is well studied and has been developed for years. However, users to date have been unwilling to adopt secure email in large numbers, due to lack of perceived need, skepticism about existing solutions, and poor usability.

The research in this proposal is transformative in that it will study both adoption and usability, identifying factors that will encourage users to employ secure email. Rather than trying to immediately scale to a global system, the research will focus on helping users gradually transition to sending secure email to their regular contacts. To make this transition simpler, the system will emphasize usability at first, with increasing security as the system is used more regularly. To further simplify adoption, interaction with encryption keys will be automated as much as possible. Usable key storage and portability will enable users to effectively manage private key material without needing to understand anything about encryption. Forward secrecy and expiring messages will mitigate damage that could be caused by a user accidentally revealing a private key or having their email account hacked.

Evaluation methods will include both two-person lab studies and long-term use "in the wild", enabling the team to evaluate whether people can adopt secure email as part of their normal email habits. Studying user behavior in a natural setting is a key to ensuring that academic results transition into practice.

Broader Impact
The broader impact of this research consists of its impact on the security community and its benefits for society and for national security. Research teams around the world will be able to contribute new key management techniques and evaluate their design on a common open source platform. By developing for email, with its generality and interoperability requirements, advances in usable key management will be broadly applicable to a wide variety of other applications, including instant messaging. National security will benefit from simple methods that government organizations can use to help their employees follow security policies for email. The PIs' research groups have a strong track record of involving undergraduate students in research, increasing the pool of students trained

in cybersecurity. One outcome of the project will be development of a module on forward secrecy and its applications in secure messaging, suitable for use in an undergraduate security course.