Multichannel Communication: Security by Network Diversity

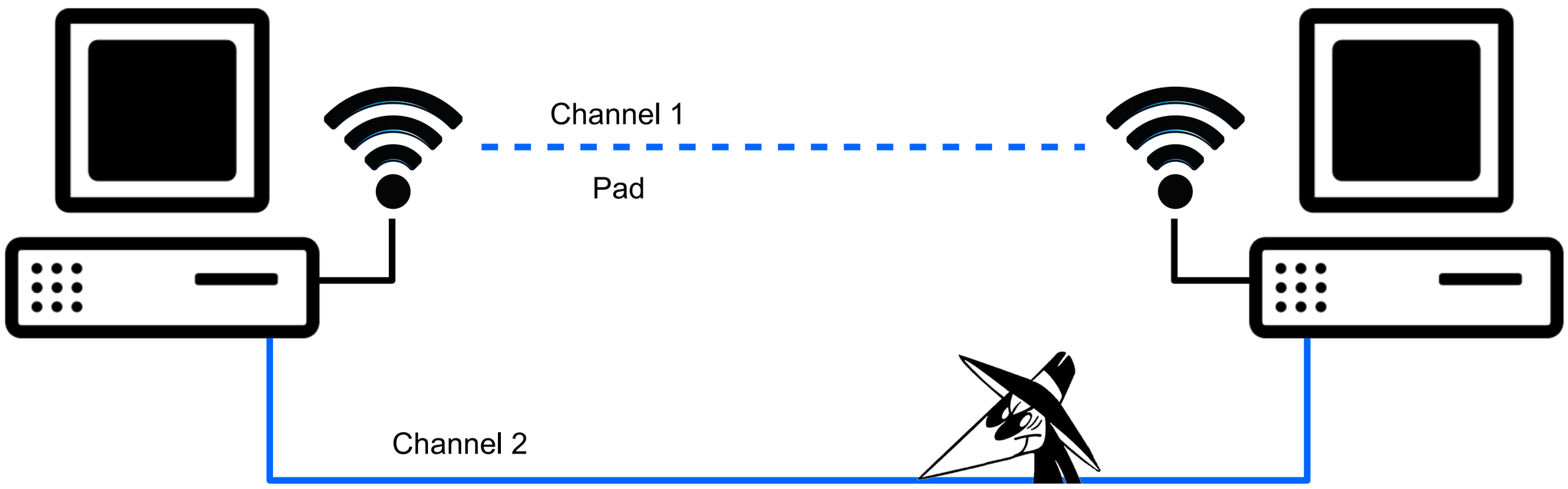
Devin J. Pohly, Patrick McDaniel

Securing end-to-end network communication has long been done by means of encryption; however, recent events and government leaks have cast doubt on the standardization and implementation of recommended cryptographic procudures. Rather than relying solely on cryptography, we propose a system that uses multichannel communication to provide additional security. In our system, an attacker must gain control of all involved networks to compromise a communication. We have implemented a proof-of-concept using a wired and wireless channel to secure data with a simple one-time pad. Proof of security then follows directly from Shannon's OTP proof. Current work involves adding cryptography for layered security and improving the overall throughput of the system. The end result will be a system which provides a form of attack resistance which derives its strength not from complex encryption but from the use of multiple networks.

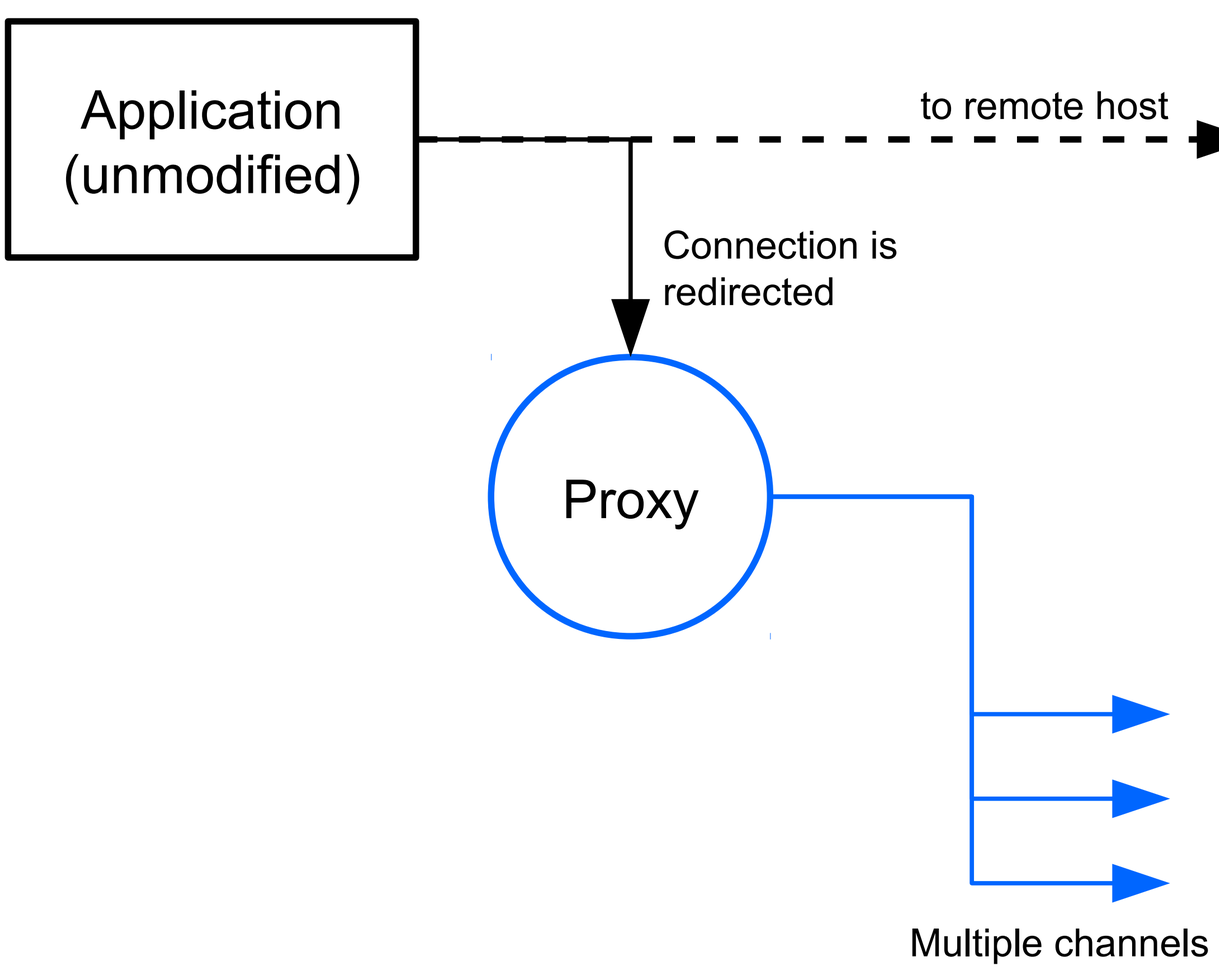
Layers of Security:

TLS
Multichannel
IPsec

End-to-End Overview



Transparent Proxy Redirection



Network Diversity

The property we exploit to provide additional security here can be called "network diversity." This is related to the concept of software diversity, which has been applied to improve the security and reliability of software systems, control systems, and other critical infrastructure. Software diversity relies on several different implementations of the same software algorithm in such a way that multple implementations must fail or be compromised to compromise the entire system. Network diversity, analogously, relies on multiple different networks in such a way that all of them must be compromised by the same attacker in order to compromise the security of a message.

Current/Future Directions

- Integration with encryption
- Addition of information/network coding for security and performance
- Improved throughput

Sponsored by the National Science Foundation