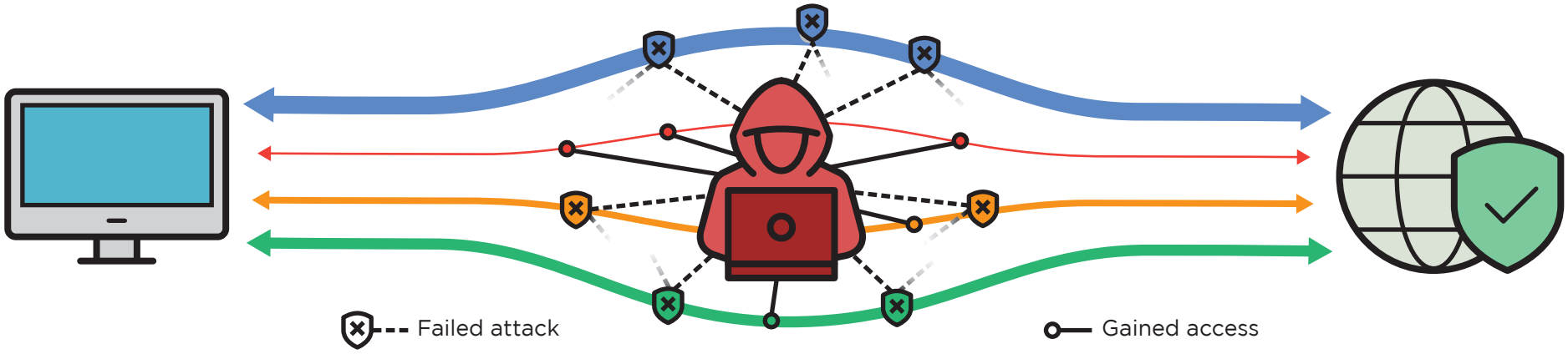
Obsolete TLS

Out-of-date TLS configurations put your data at risk

Attackers can exploit outdated transport layer security (TLS) protocol configurations to gain access to sensitive data with very few skills required. The graphic below depicts network traffic flows with various configurations, in an abstract manner. Updating TLS configurations to use strong encryption and authentication will help provide organizations with the cryptographic agility to stay ahead of malicious actors' capabilities and protect important information.



Network Traffic Encryption Types

- ⚠ **Data at risk** Obsolete TLS
- **Data may be at risk** Authorized TLS with weak cipher suite
- **Data may be at risk** Authorized TLS with compliant cipher suite
- **Data protected** Authorized TLS with compliant cipher suite and strong key exchange methods

Data at Risk: Common types of data sent over TLS

- Proprietary information
- Network sensitive files
- Web traffic using HTTPS
- Social security numbers
- Passwords
- Travel information
- Online payment information
- Other sensitive files

For more information on how to detect, prioritize, and remediate network components using outdated TLS, refer to NSA's cybersecurity product "Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations" available on **NSA.gov/cybersecurity** and sample configurations and network signatures on the **NSA Cybersecurity GitHub**.