



# Hacking Windows Vista Security

Dan Griffin  
JW Secure, Inc.



# Introduction

- Who am I?
- What are these tools and where did they come from?



# Topic Summary

- Sample code projects are C/C++ based & require Vista
- Free downloads!
- Topics: Crypto, Firewall, IPsec

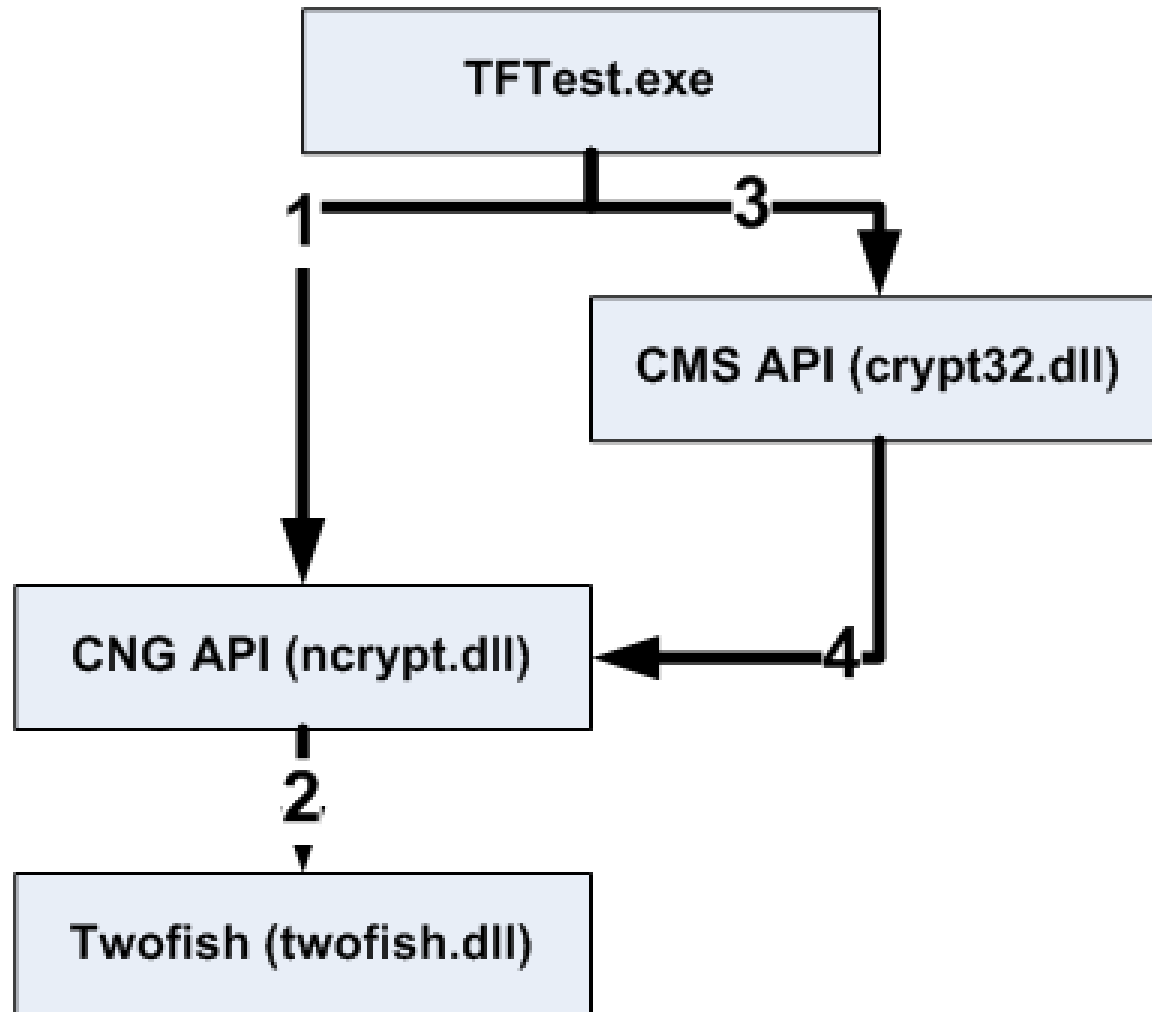


# Hacking Crypto

- What's CNG?
- What's CMS?
- What's Twofish?
- Article link
  - <http://blogs.msdn.com/onoj/archive/2007/05/10/window>
- Code download
  - <http://download.microsoft.com/download/f/1/2/f12dbbb>



# Twofish Plug-in Architecture





# Crypto Demo

(Or, now NSA can't read my email 😊)

(maybe ...)



# Hacking The Firewall

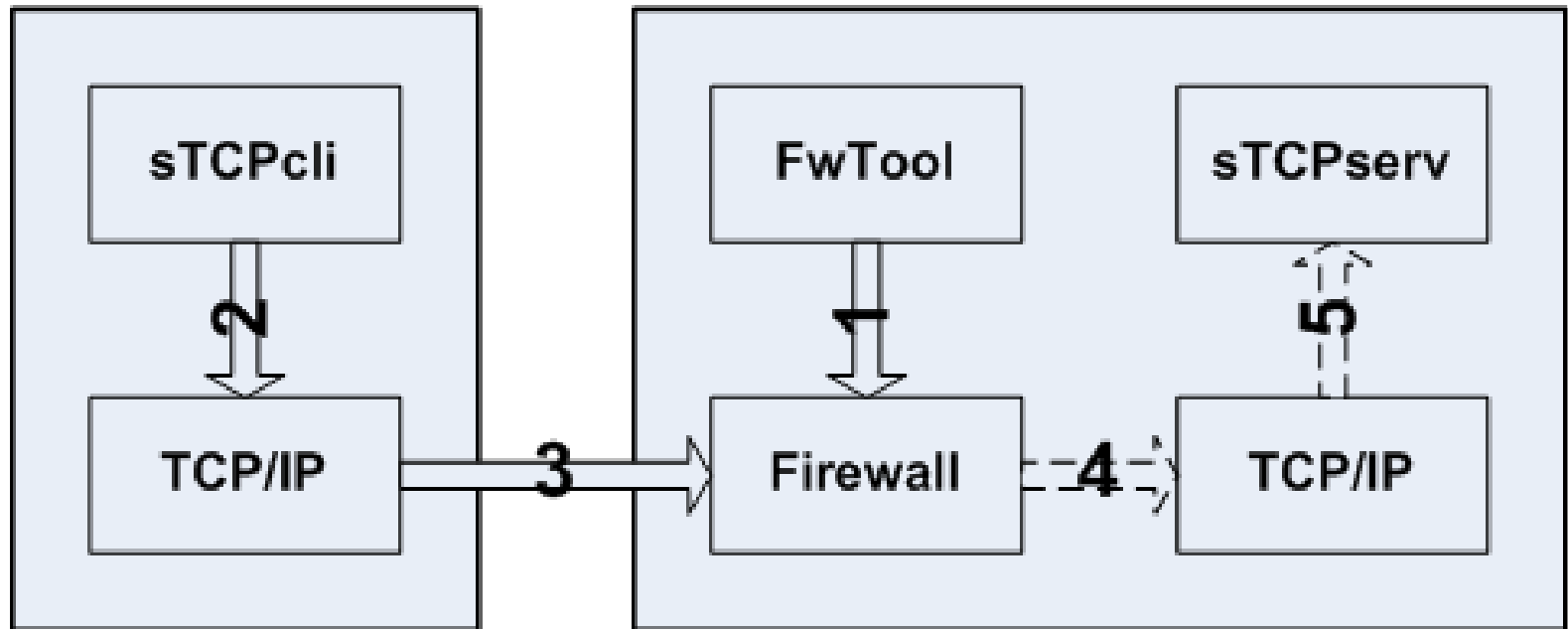
- What's a network firewall?
- Article link
  - <http://blogs.msdn.com/onoj/archive/2007/05/09/window>
- Code download
  - <http://download.microsoft.com/download/f/1/2/f12dbbb>



# FwTool Architecture

Workstation (A) – Socket Client

Workstation (B) – Socket Listener





# Firewall Demo



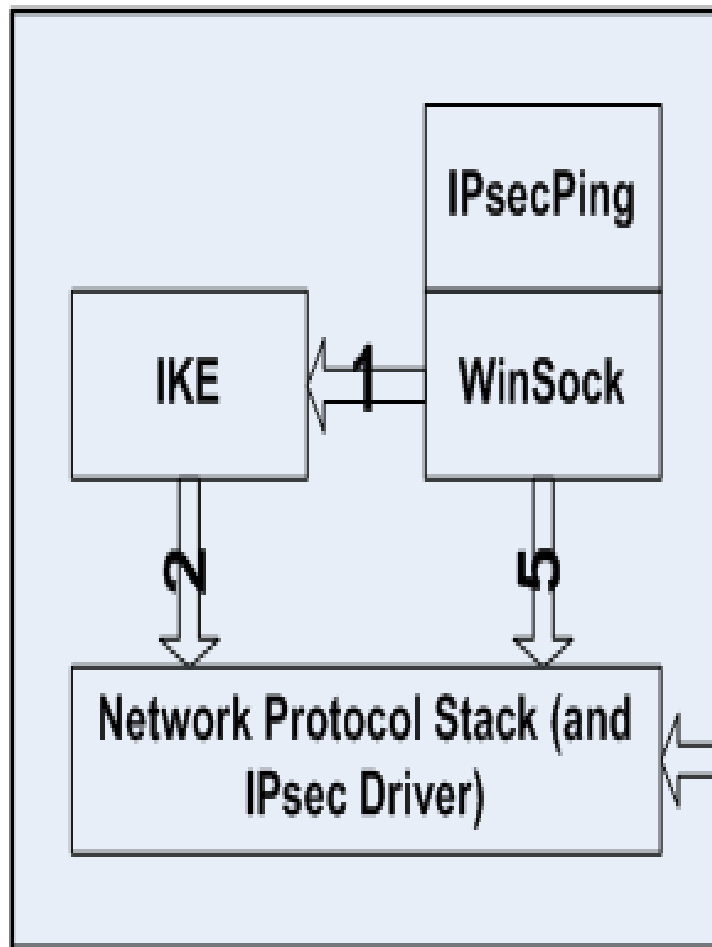
# Hacking IPsec/Socket Extensions

- What's IPsec?
- What's "Winsock Secure Socket Extensions"?
- Code download
  - <http://download.microsoft.com/download/f/1/2/f12dbbb>

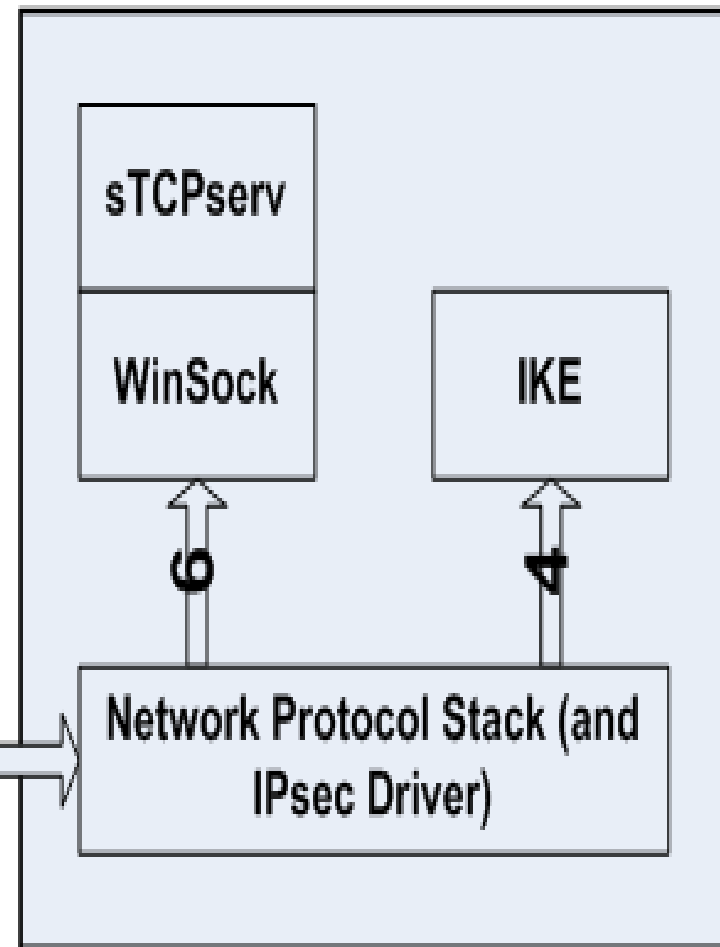


# IPsecPing Architecture

Workstation (A) – Socket Client



Workstation (B) – Socket Listener





# IPsecPing Demo

- (Co-developed with V6 Security, Inc.)



# Questions?

- Contact Info
  - Dan Griffin ([dan@jwsecure.com](mailto:dan@jwsecure.com))
  - Blog = <http://www.jwsecure.com/dan/>