

# Project **Doppelgänger**

## Cyber Security Division 2012 Principal Investigators' Meeting

Oct 10<sup>th</sup>, 2012

Salvatore J. Stolfo & Ang Cui  
Principal Investigator & Graduate Researcher  
Columbia University  
[{sal|ang}@cs.columbia.edu](mailto:{sal|ang}@cs.columbia.edu)  
212-939-7080

# Doppelgänger Introduction

- TTA 6 – Modeling of Internet Attacks

# Doppelgänger Introduction

- TTA 6 – Modeling of Internet Attacks
  - Monitoring of Attacks against the Internet Infrastructure

# Doppelgänger Introduction

- TTA 6 – Modeling of Internet Attacks
  - Monitoring of Attacks against the Internet Infrastructure
  - Monitoring of Attacks against

# Doppelgänger Introduction

- TTA 6 – Modeling of Internet Attacks
  - Monitoring of Attacks against the Internet Infrastructure
  - Monitoring of Attacks against
    - Networked Embedded Devices

# Doppelgänger Introduction

- TTA 6 – Modeling of Internet Attacks
  - Monitoring of Attacks against the Internet Infrastructure
  - Monitoring of Attacks against
    - Networked Embedded Devices
    - Proprietary hardware & software

# Doppelgänger Introduction

- TTA 6 – Modeling of Internet Attacks
  - Monitoring of Attacks against the Internet Infrastructure
  - Monitoring of Attacks against
    - Networked Embedded Devices
    - Proprietary hardware & software
    - Non-standard operating systems

# Doppelgänger Introduction

- TTA 6 – Modeling of Internet Attacks
  - Monitoring of Attacks against the Internet Infrastructure
  - Monitoring of Attacks against
    - Networked Embedded Devices
    - Proprietary hardware & software
    - Non-standard operating systems
    - Closed systems with “no” way of hosting third-party code

# Doppelgänger Introduction

- TTA 6 – Modeling of Internet Attacks
  - Monitoring of Attacks against the Internet Infrastructure
  - Monitoring of Attacks against
    - Networked Embedded Devices
    - Proprietary hardware & software
    - Non-standard operating systems
    - Closed systems with “no” way of hosting third-party code
    - Resource constrained devices running (**very**) legacy code

# Doppelgänger Introduction

- TTA 6 – Modeling of Internet Attacks
  - Monitoring of Attacks against the Internet Infrastructure
  - Monitoring of Attacks against
    - Networked Embedded Devices
    - Proprietary hardware & software
    - Non-standard operating systems
    - Closed systems with “no” way of hosting third-party code
    - Resource constrained devices running (very) legacy code
  - Individual devices that make up the Internet substrate

# Doppelgänger Approach

- Some motivation...

## **23. Are current HP multifunction printers susceptible to viruses and worms?**

No, since the majority of viruses and worms exploit vulnerabilities in Windows-based computers. HP MFPs use non-standard operating systems other than Windows. Consequently, they are immune to these viruses and worms. In practice, there have been no known instances of viruses or worms infecting HP MFPs.

In the future HP will likely ship MFPs which include an embedded version of the Windows operating system. However, there are a number of practical reasons why this won't increase the security risk faced by customers.

# Doppelgänger Approach

- Some motivation...



4. Win: Reverse Shell  
Server -> Kitteh

Firewall

Network Printer

se Proxy



# Doppelgänger Approach

- Some motivation...

## H(ackers)\_2O: Attack on City Water Station Destroys Pump

By Kim Zetter  November 18, 2011 | 2:02 am | Categories: Breaches, Cybersecurity, Hacks and Cracks

 Follow @KimZetter

615

52

116

 Tweet

 +1



 Like

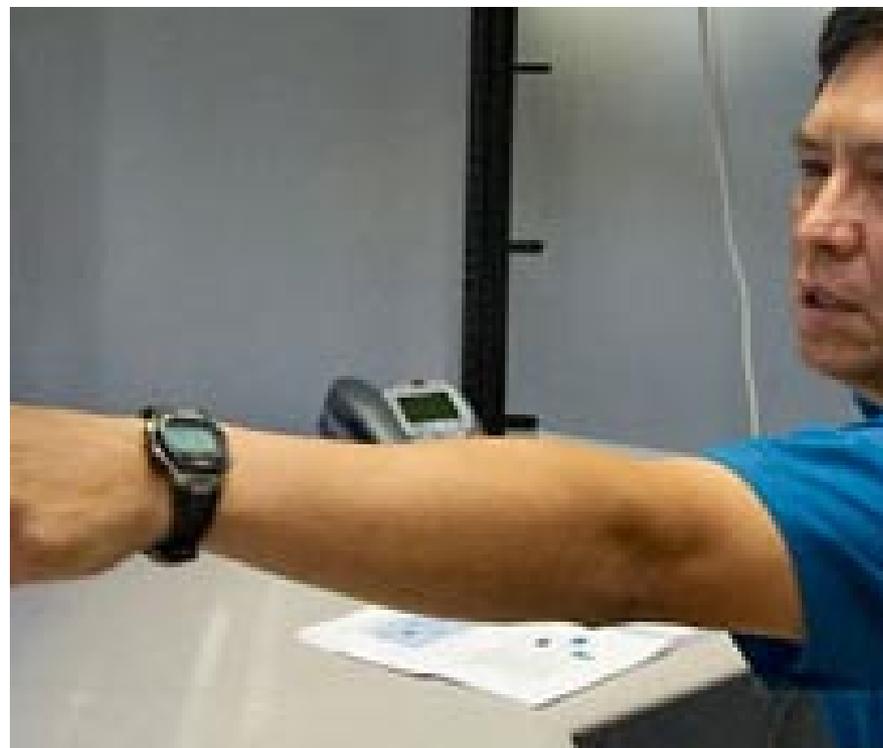
 Send

 804 people like this.



# Doppelgänger Approach

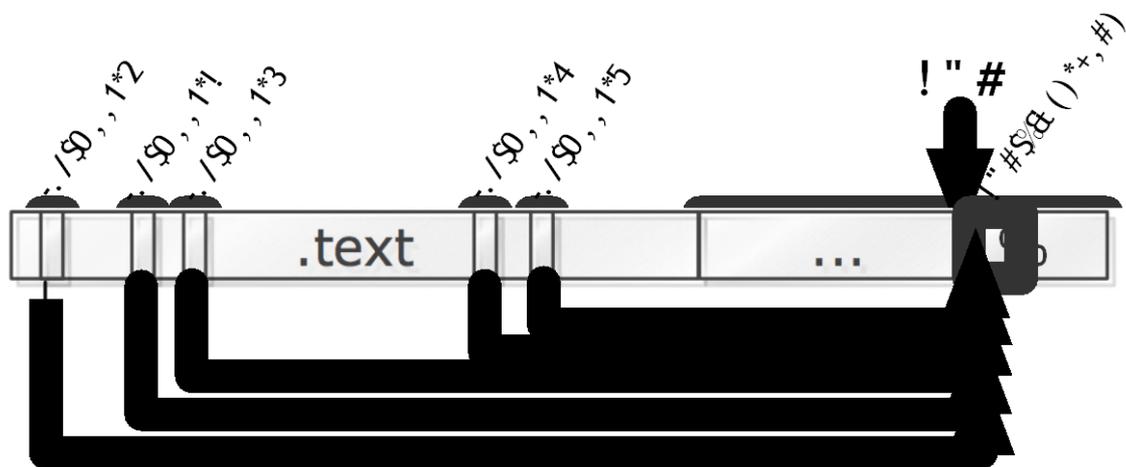
- Some motivation...



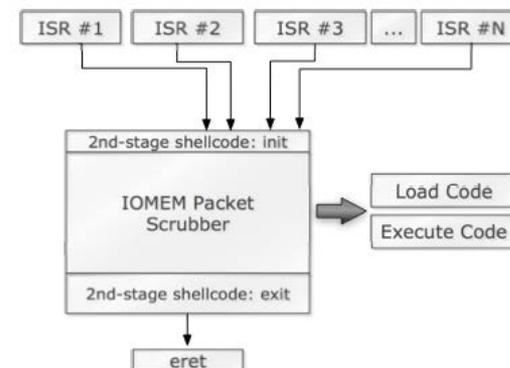
# Doppelgänger Approach

- Some motivation...

## Version Agnostic Cisco IOS Rootkit



- the (mips) ERET, or Exception-Return is an architecture invariant
- ISR **entry** point is a **binary** invariant, typically found at 0x600080180, etc
- Can just hijack entry point, but there is an ulterior motive
- Use ERET locations in the image to **fingerprint** IOS version



# Doppelgänger Approach

- Challenges
- Undocumented, proprietary OS & hardware
- Over 300,000 firmware images in the wild
- “No” mechanism to run third-party code
- No host-based defense
- Resource-constrained, real-time environment

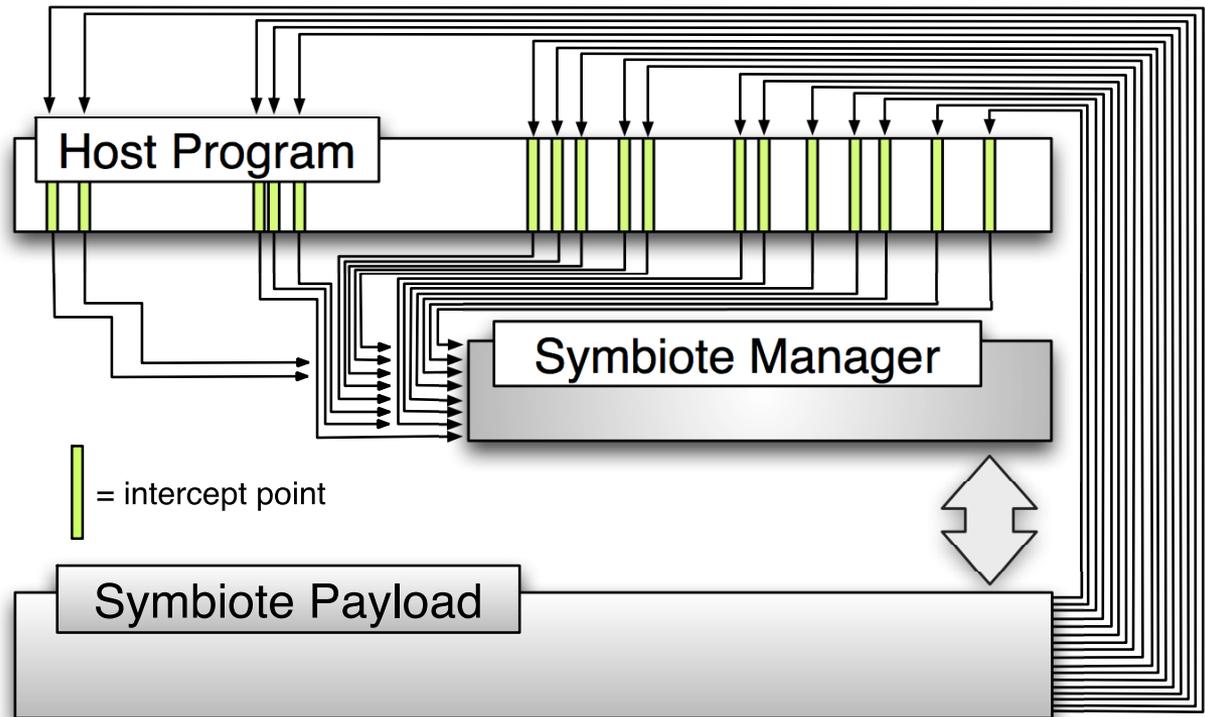


# Doppelgänger Approach

- Proposed Technical Approach
  - Novel code injection platform that embeds intrusion detection function into legacy routers
  - Demonstration of host-based intrusion detection functionality on different router platforms
  - Test @ DETER
- Cisco IOS prototype now exists
- Doppelgänger code injection ported to FRAK
- FRAK: Firmware Reverse Analysis Konsole

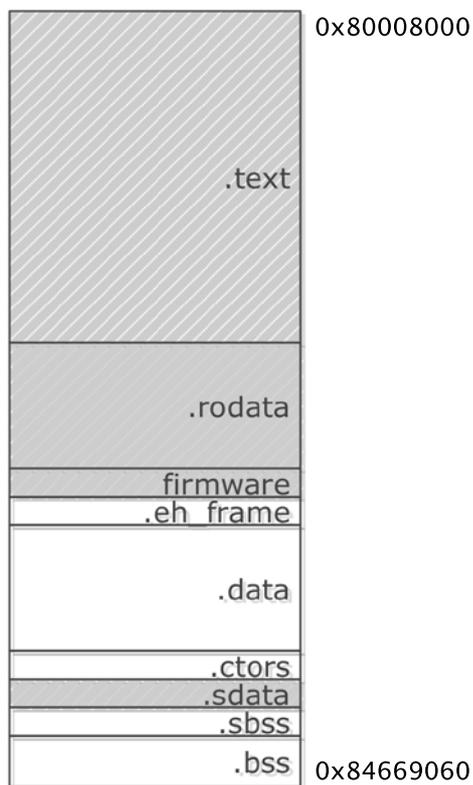
# Doppelgänger Approach

- Doppelgänger



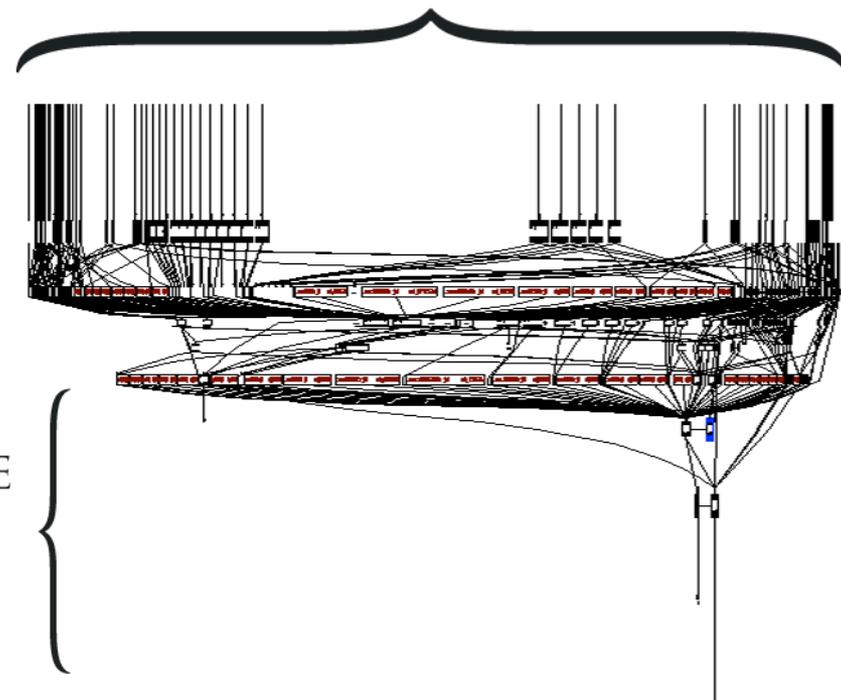
# Doppelgänger Approach

- Fortifying Cisco IOS



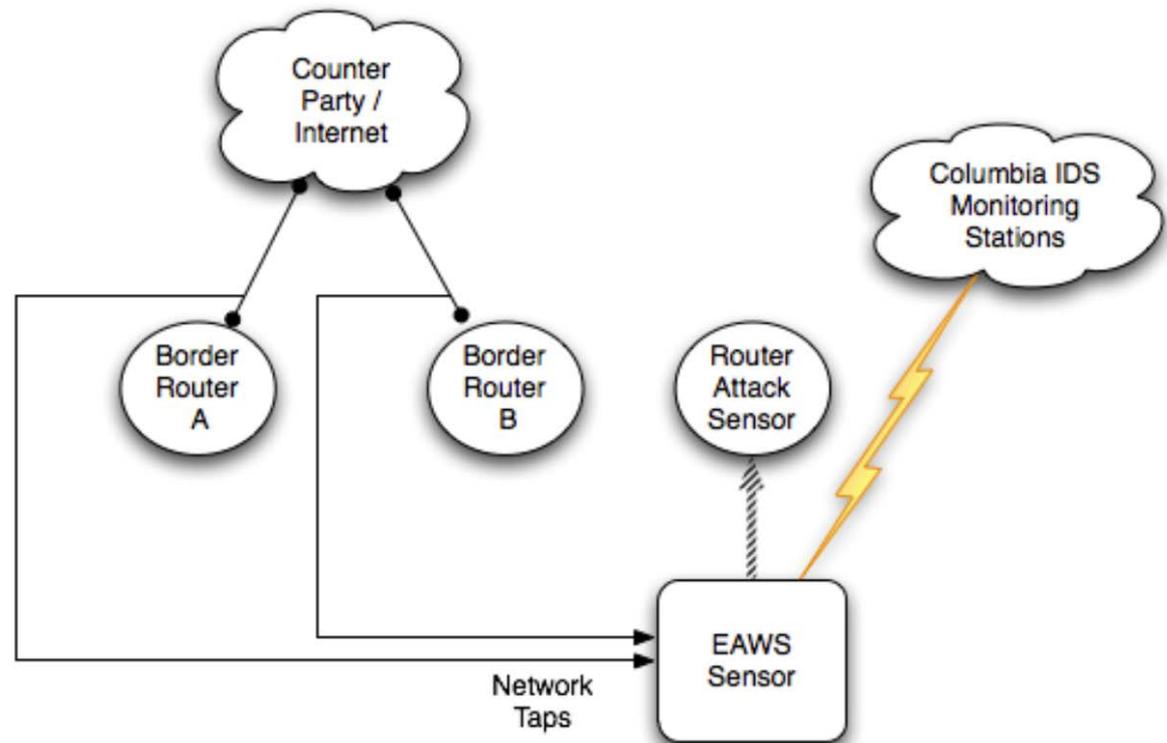
 = Static Regions

## CONTROL-FLOW INTERCEPTS



# Doppelgänger Approach

- EAWS: Early Attack Warning System



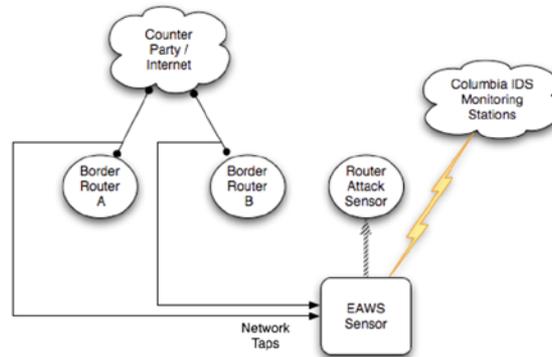
# Doppelgänger Milestones

- Emulator-based Sensor
  - Test function and safety on the network
- Physical router Sensor
  - Test latency
- Alert reporting infrastructure
  - Stealth channels & Open channels
- Develop exploits and attacks
- Test and Evaluation
  - Columbia network
  - DETER testbed
- Do not be late with monthly reports

# Doppelgänger Tech Transfer

- Red Balloon Security Inc.
  - FRAK will be available soon.
  - In discussion with large embedded & AV vendors.

# Doppelgänger Quad Chart



## Operational Capability:

1. Real-time Detection of Malware attacks against Routers
2. Millisecond detection rate
3. Low cost sensors, no impact on operational environments
4. A new capability to detect attacks against critical routers, a technology not available today

## Proposed Technical Approach:

1. A novel code injection platform that embeds intrusion detection function into legacy routers
2. Implementation of a range of legacy routers converted to sensors and tested at DETER
3. CISCO IOS platform prototype is now demonstrable
4. Doppelgänger code injection platform being ported to several other platforms
5. Ongoing research at the Columbia IDS lab on malware detection

Professor Salvatore J Stolfo  
Department of Computer Science  
Columbia University  
Mail Code 0401  
1214 Amsterdam Avenue  
New York, NY 10027  
212-939-7080 (v)  
212-666-0140 (fax)  
[sal@cs.columbia.edu](mailto:sal@cs.columbia.edu)

# Doppelgänger Questions

- Contact:
  - [Sal@cs.columbia.edu](mailto:Sal@cs.columbia.edu)
  - [Ang@cs.columbia.edu](mailto:Ang@cs.columbia.edu)