CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

Advanced Situation Awareness of High Impact Malware Attacks Against the Internet Routing Infrastructure

Columbia University and Red Balloon Security, Inc.

Ang Cui

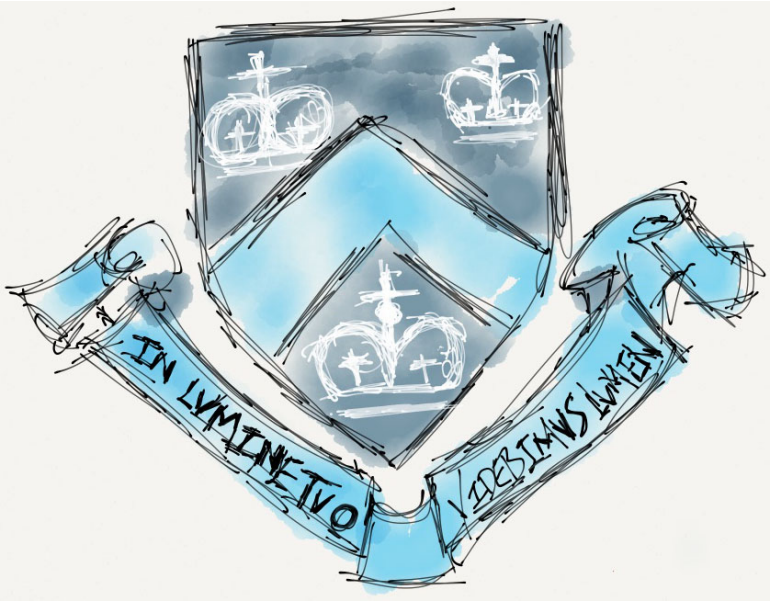
Wednesday Sept 18 1155am

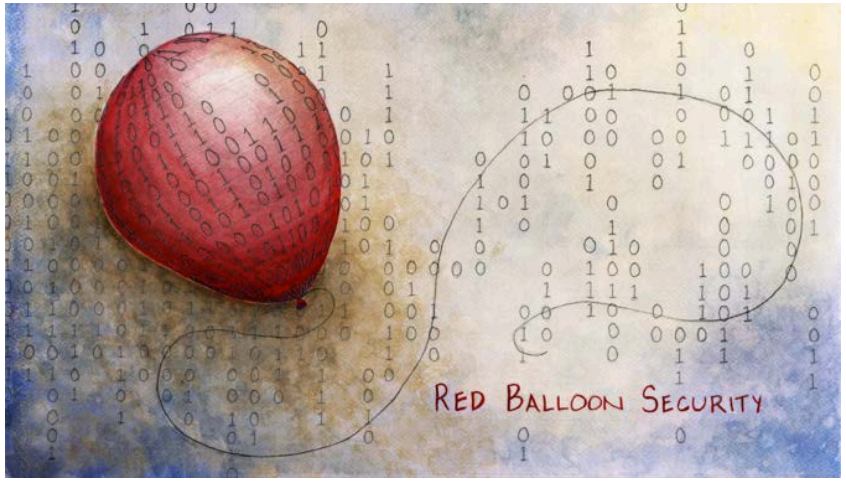
Homeland Security

Science and Technology

Team Profile

- Red Balloon Security is the exclusive licensee of Columbia's Symbiote Technology
  - Developed in the IDS Lab of Columbia University





Team Profile

- Red Balloon Security is the exclusive licensee of Columbia's Symbiote Technology
  - Developed in the IDS Lab
- RBS has demonstrated successful exploitation of printers, routers and IP Phones

Team Profile

- Red Balloon Security is the exclusive licensee of Columbia's Symbiote Technology
  - Developed in the IDS Lab
- RBS has demonstrated successful exploitation of printers, routers and IP Phones
- RBS has developed commercial grade versions of Symbiote Technology

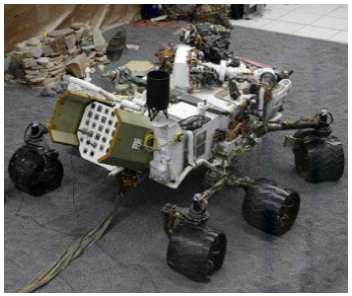
Team Profile

- Red Balloon Security is the exclusive licensee of Columbia's Symbiote Technology
  - Developed in the IDS Lab
- RBS has demonstrated successful exploitation of printers, routers and IP Phones
- RBS has developed commercial grade versions of Symbiote Technology
- RBS has produced the world's first Embedded Device "AV" for
  - Cisco IOS Routers, Printers, IP Phones, …

Billions of Embedded Systems with no Anti-Virus
(We have to break them to learn how to fix them)

50 Million - Hacked

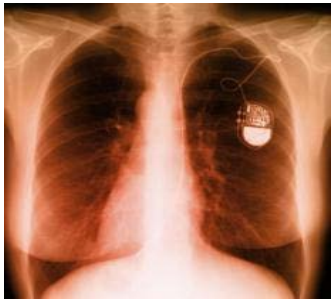
Hacked



3? Hacked???

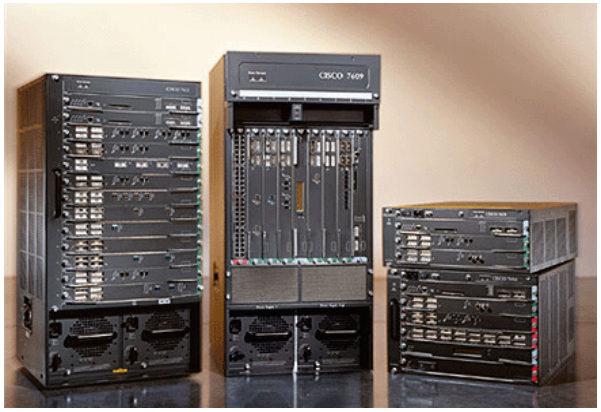
100 Million/year - Hacked

How many? Hacked



Millions? (Unknown due to HIPPA)

Runs our homes
70 Million - Hacked



Runs the internet! Hacked

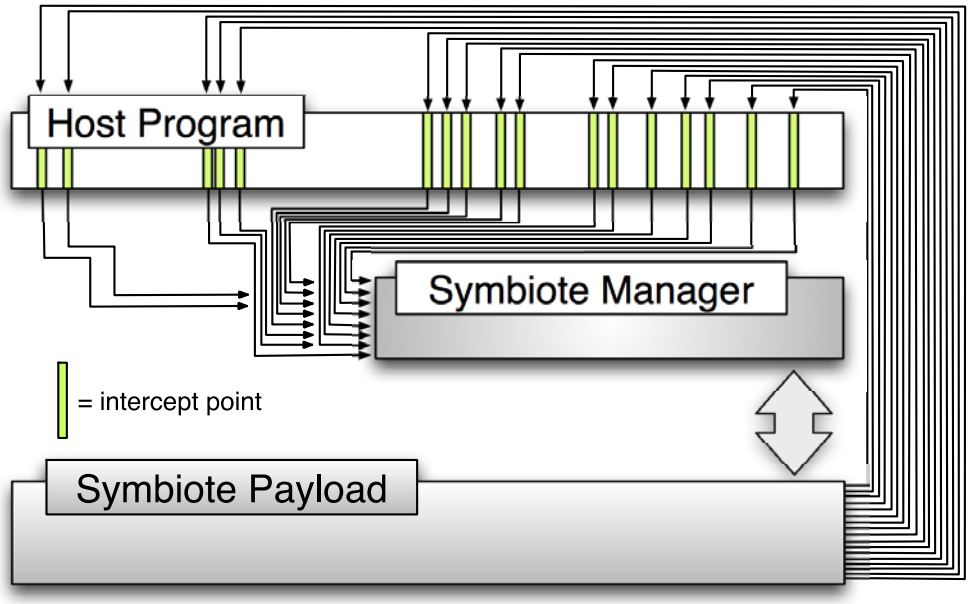
Customer Need

- Embedded devices are insecure

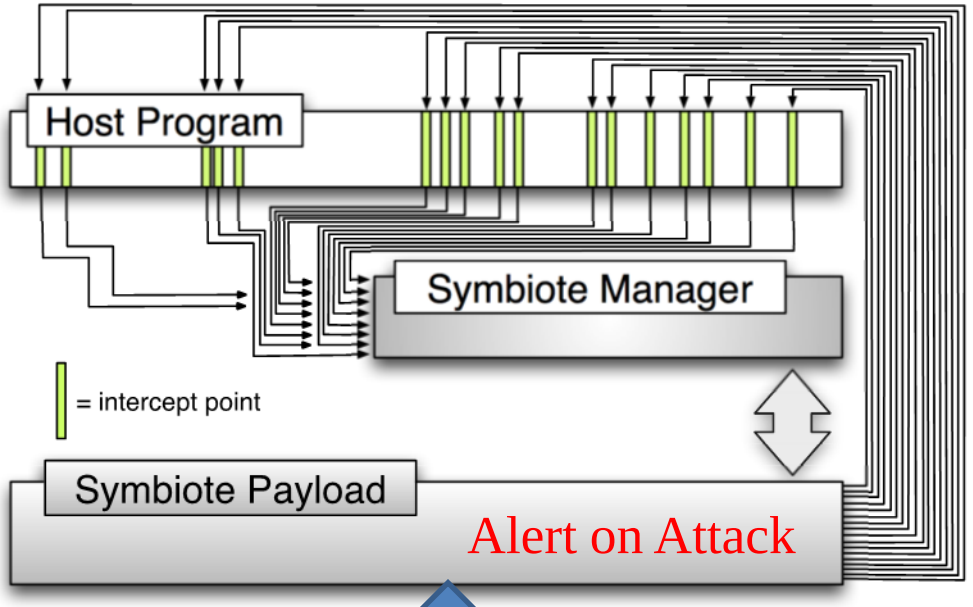
- The myriad of different ISA's, OS's, Proprietary Firmware versions makes it all but impossible to develop a single security solution until now
- Symbiote technology was invented to inject security functionality in arbitrary firmware
  - Injection is "randomized" - Self-protecting
  - Automated through FRAK

Approach

Defending Embedded Systems with Software Symbiotes



Converting Symbiote-injected Routers into Network Attack Detectors



EAWS Sensor
Early Attack Warning Sensor

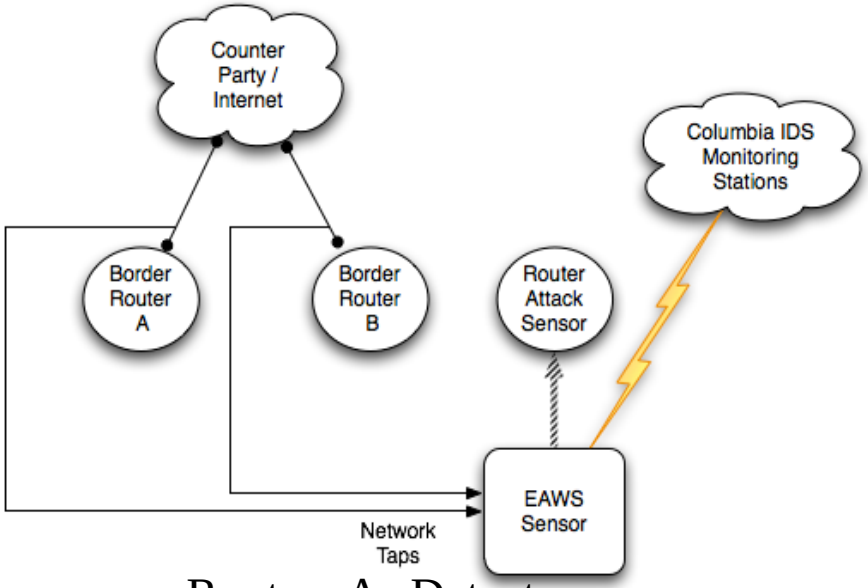
Cisco Router

Benefits

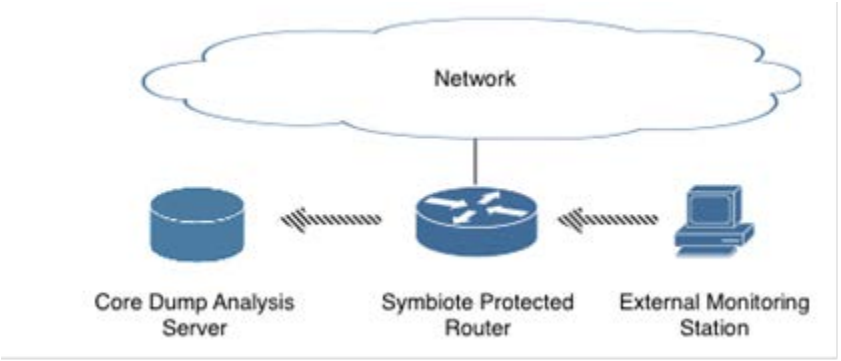
- All embedded devices can now be protected from advanced malware threats

- The internet routing infrastructure can also be turned into a monitoring infrastructure to detect advanced threats

Early Attack Warning System against the Routing Infrastructure



Routers As Detectors



Easy Deployment Anywhere

- No impact on network operations
- Integrated with existing SIMs
- New eyes into the security posture of the network

Competition

- None, really! (Except perhaps inertia to do nothing)

Current Status

- Testable Symbiote-protected Cisco IOS router ready for test and evaluation at Deter within 6 months

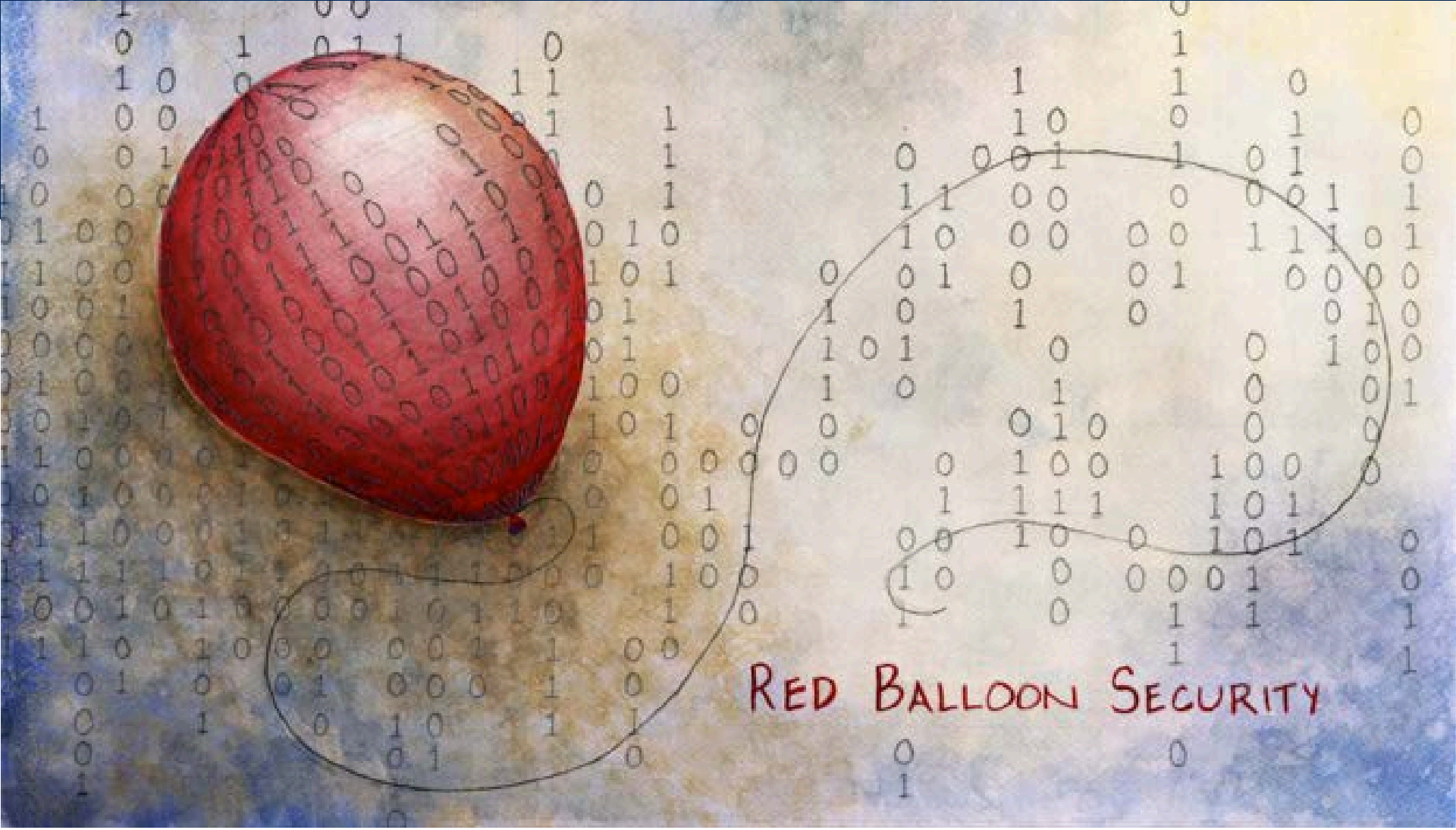
Next Steps

- Complete T&E and deliver Symbiote-protected router sensor
- RBS successfully transitioned technology from Columbia and is in direct discussions with vendors

Contact Information

- Salvatore Stolfo – PI
  - Professor, Columbia University
    - sal@cs.columbia.edu
  - Director, Red Balloon Security
    - s@redballoonsecurity.com

- Ang Cui
  - Senior GRA, Columbia University
    - ang@cs.columbia.edu
  - CEO, Red Balloon Security
    - a@redballoonsecurity.com



sal@cs.columbia.edu
sal@redballoonsecurity.com

ang@cs.columbia.edu
ang@redballoonsecurity.com