RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: BR-T08

Embedded Exploitation Party Trick!

Ang Cui

Ph.D.
Columbia University
Chief Scientist, Red Balloon

Who I am, What I Do

Ang Cui

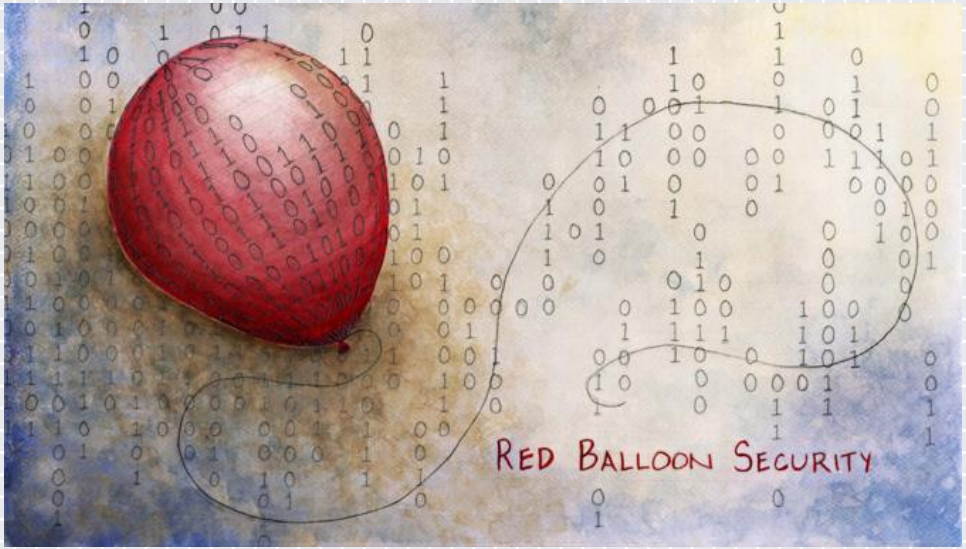
Who I am, What I Do

DR. Ang Cui !

Who I am, What I Do

Co-founder,
Chief Scientist

Red Balloon Security



Who I am, What I Do

Security Researcher

TIME Subscribe

SECURITY

Set Your Printer on Fire? Hackers Can Do What?

By Matt Peckham @mattpeckham | Nov. 30, 2011 | Add a Comment

Share Like 89 Tweet 239 +1 5 Share 22 Pin it

Read Later

Imagine: Your printer, at rest in your home office as you're away at work or maybe out shopping. Suddenly it powers up, humming, making that familiar mechanical shuffling sound so many printers emit during startup. But after a

IEEE SPECTRUM

Follow on:

Topics Reports Blogs Multimedia Magazine Resources

News | Computing | Embedded Systems

Embedded Anti-Malware Defends Against Cisco IP Phone Hack

Software "symbiotes" signal attacks on embedded systems

By Charles Q. Choi
Posted 27 Feb 2013 | 21:00 GMT

Share | Email | Print

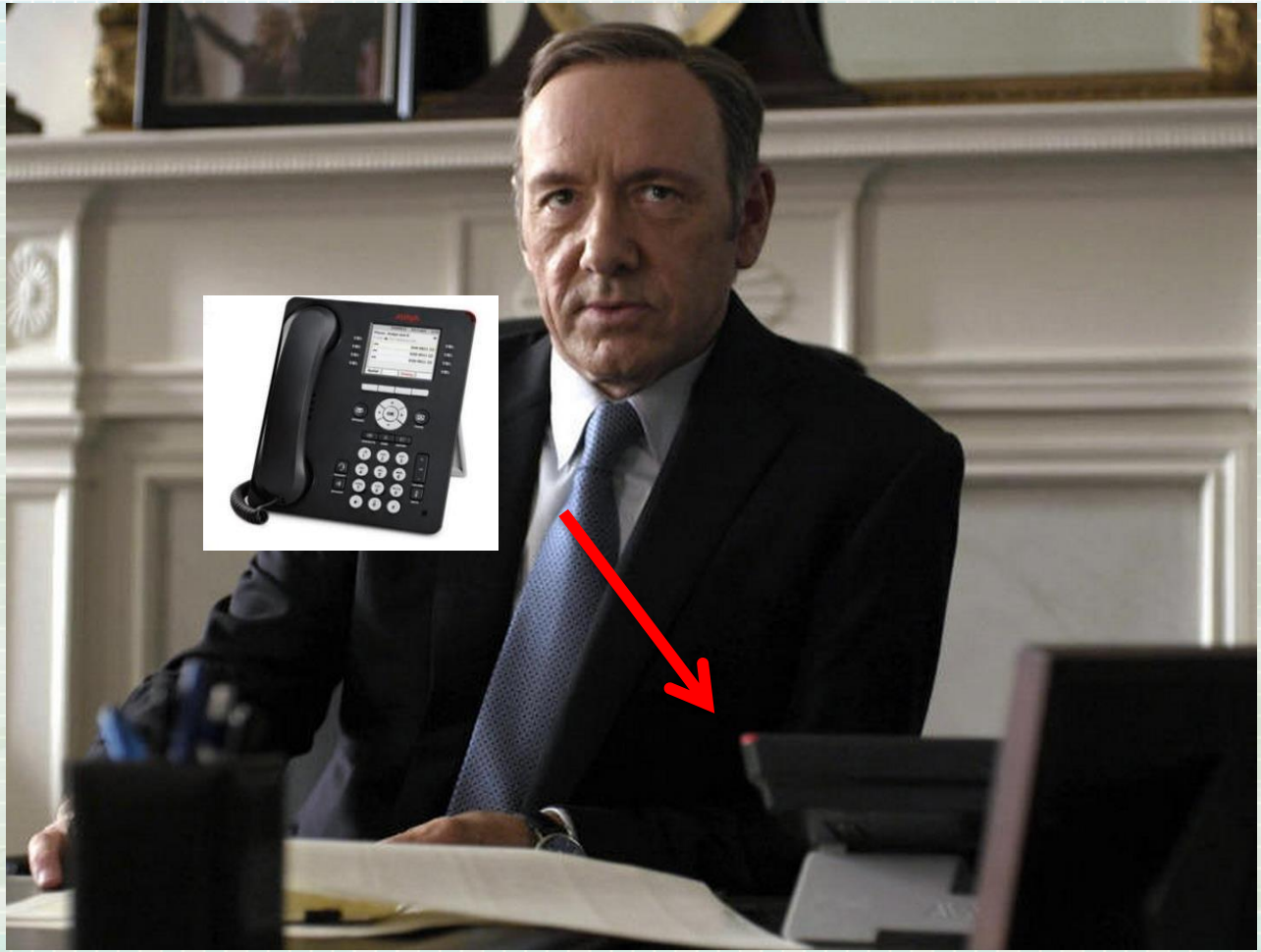
All current Cisco IP phones, including the ones seen on desks in the White House and aboard *Air Force One*, have a vulnerability that allows hackers to take complete computer

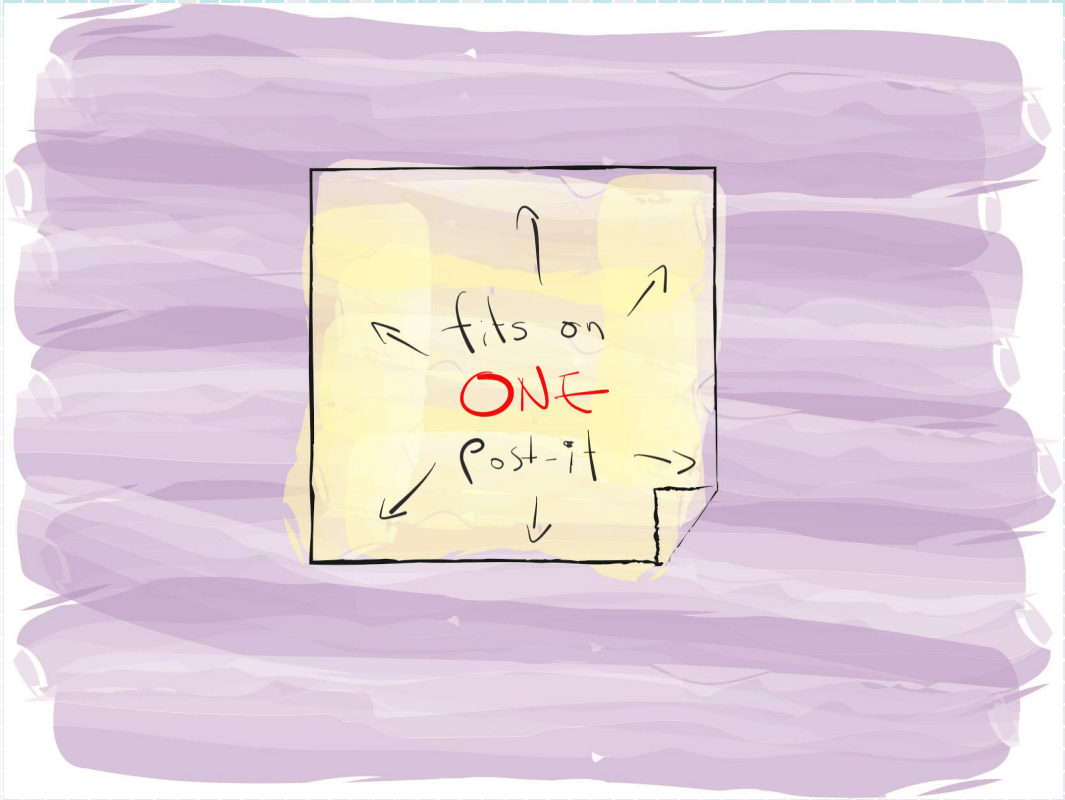
Related Stories

Great stories start in mid-drama

@ RSA_2014

My friend,
the Avaya ONE-X phone (9608)





ASA-2014-099

RELEASED 2014

PSN #	PSN004154u				
Original publication date: 27-Feb-14. This is Issue #01, published date: 27-Feb-14.		Severity/risk level	Medium	Urgency	when convenient
Name of problem	Avaya 96x1 and B189 Endpoint Command Injection, Memory Modification and Code Execution Vulnerabilities				
Products affected					

Avaya IP Endpoints affected:

Product:	**Affected Version(s):**	**Risk Level:**	**Actions:**
Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones	6.3.1.21 and earlier SIP software	Medium	Upgrade to SIP software release 6.3.1.22 or later.
Avaya 9608/9608G/9611G/9621G/9641G IP Deskphones	6.3.1.51 and earlier H.323 software	Medium	Upgrade to H.323 software release 6.3.1.52 or later.

Avaya 9608 Vulnerability # 2

Vulnerability Details will not be published until we all…

https://downloads.avaya.com/css/P8/documents/100178648

Avaya 96xx Security Analysis

- accidentally found this Exploit

… while trying to exploit another Exploit…

Avaya 96xx Security Analysis

- Challenged by Avaya representative at NTSWG briefing on Cisco Endpoint Exploitation

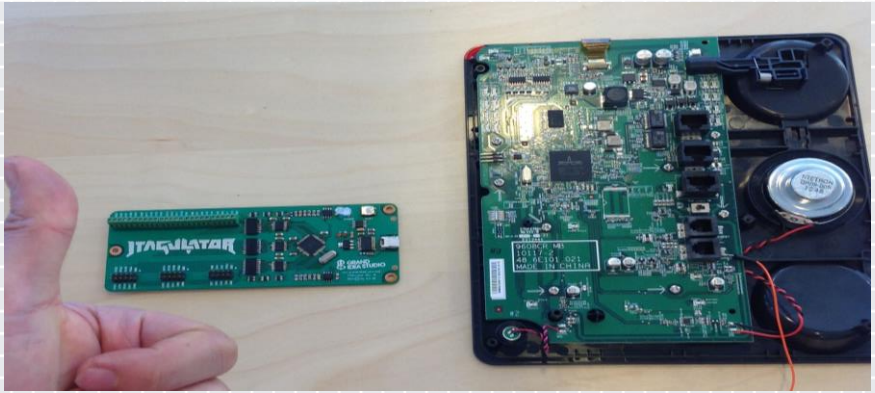
Avaya 96xx Security Analysis

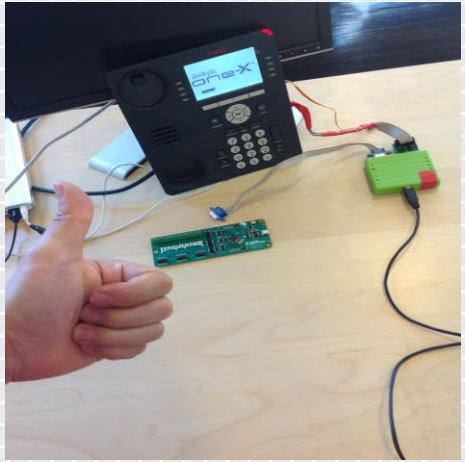
- Challenged by Avaya representative at NTSWG briefing on Cisco Endpoint Exploitation

- Challenge (eventually) accepted

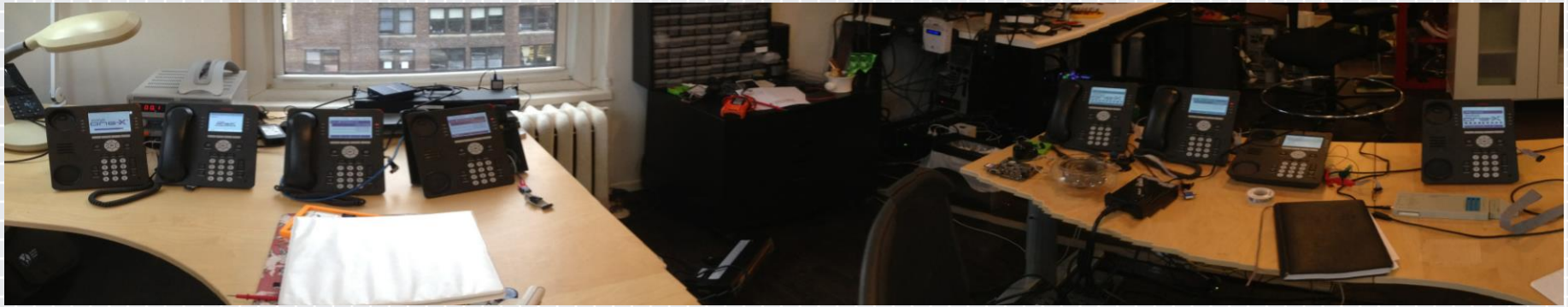
Avaya 96xx exploitation process

- Initial penetration
  - Difficult
  - Nearly zero attack surface without avaya environment
  - Resorted to physical tear-down



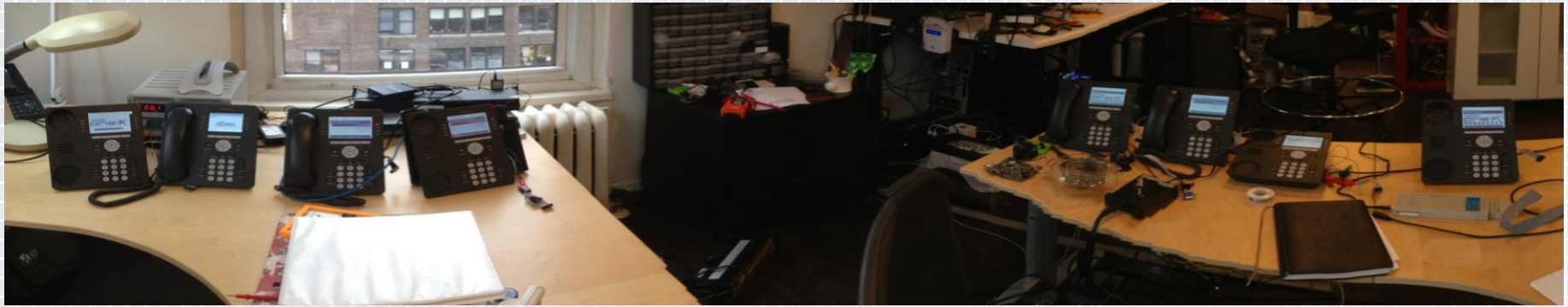


Avaya 96xx exploitation process



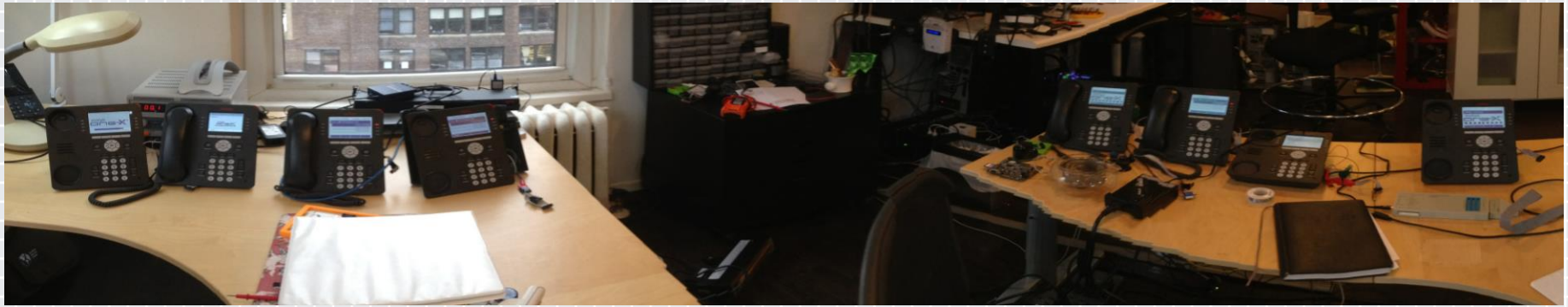
- 20 phone fuzz farm

Avaya 96xx exploitation process



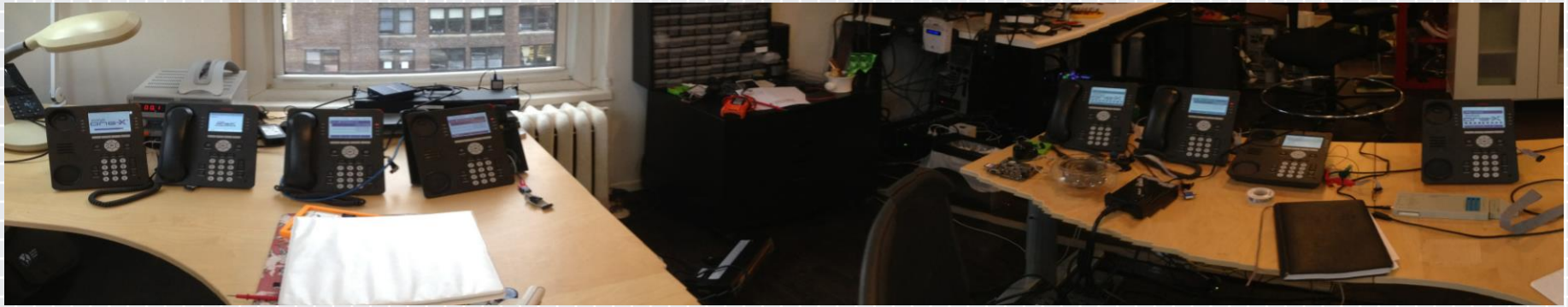
- 20 phone fuzz farm
- 1 month automated fuzzing

Avaya 96xx exploitation process



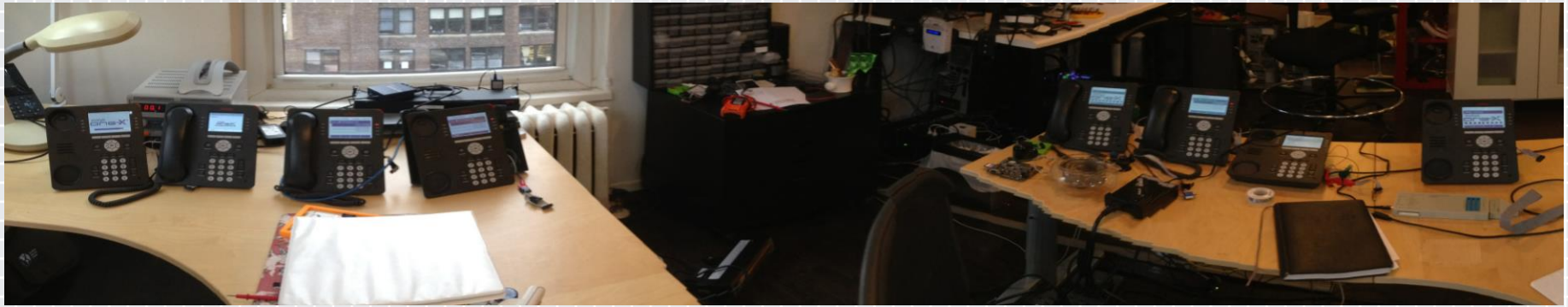
- 20 phone fuzz farm
- 1 month automated fuzzing
- 10gb of crash data

Avaya 96xx exploitation process



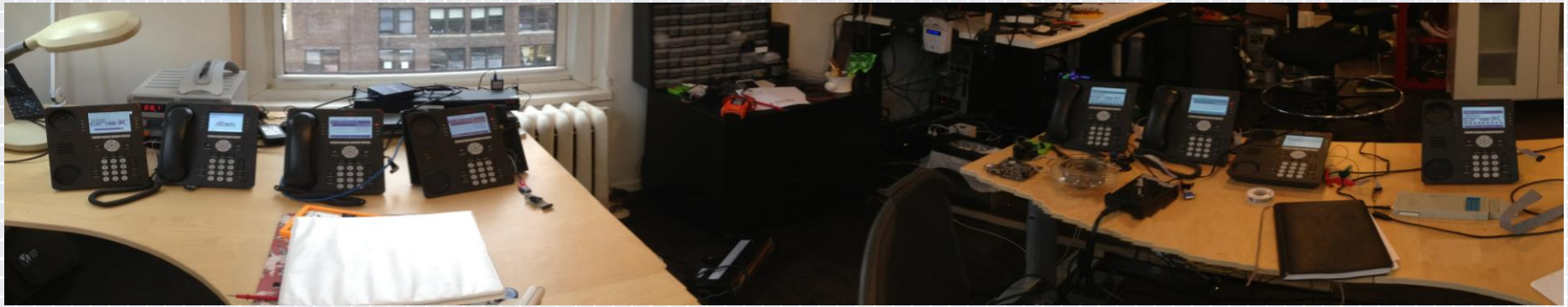
- 20 phone fuzz farm
- 1 month automated fuzzing
- 10gb of crash data
- 10K+ documented crashes

Avaya 96xx exploitation process



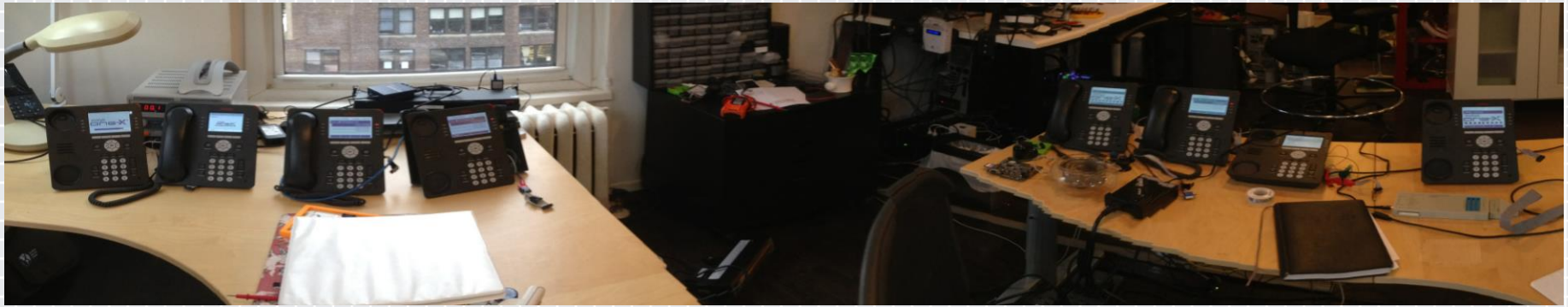
- 20 phone fuzz farm
- 1 month automated fuzzing
- 10gb of crash data
- 10K+ documented crashes
- Ran basic clustering algorithm to determine unique root-causes

Avaya 96xx exploitation process



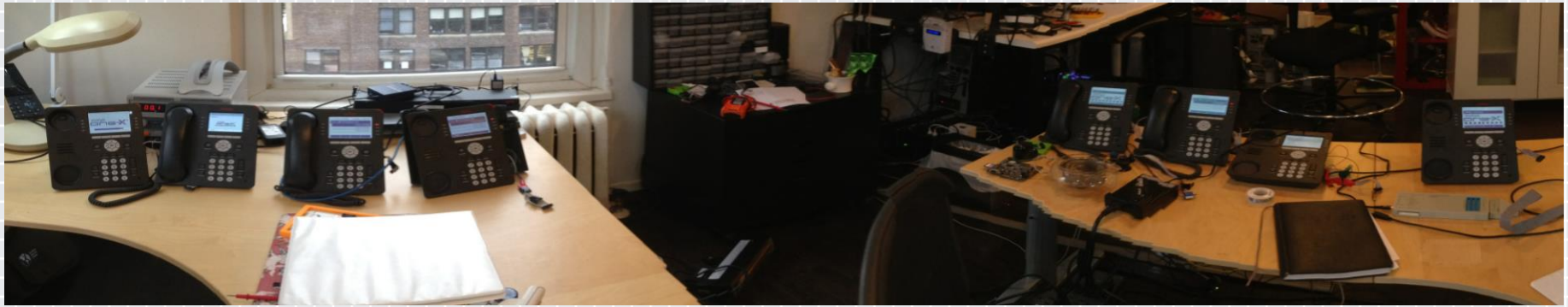
- Chose top 4 unique crash cases

Avaya 96xx exploitation process



- Chose top 4 unique crash cases
- All Reliably reproducible

Avaya 96xx exploitation process



- Chose top 4 unique crash cases
- All Reliably reproducible
- Manual analysis for exploitability

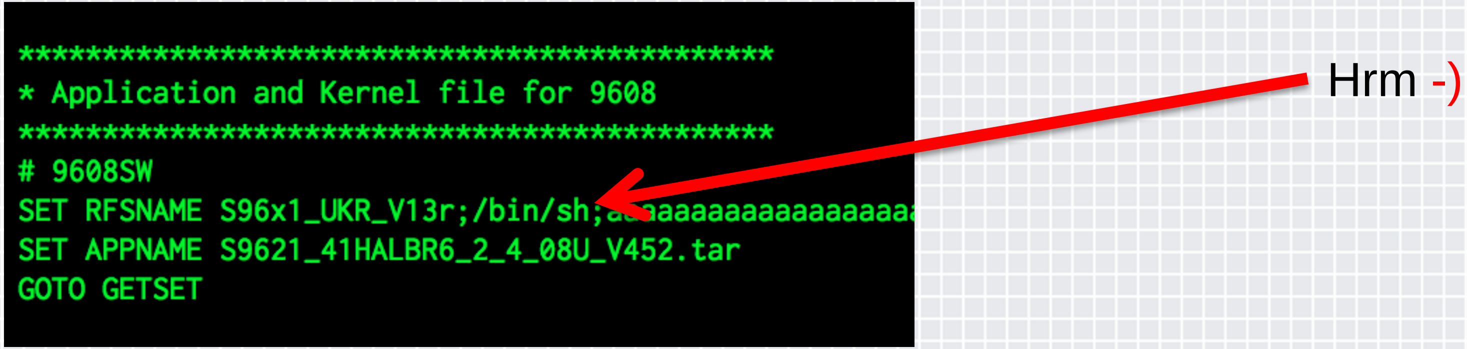
p3wn like it's 1998!

```
**********************************************
* Application and Kernel file for 9608
**********************************************
# 9608SW
SET RFSNAME S96x1_UKR_V13r58_V13r58.tar
SET APPNAME S9621_41HALBR6_2_4_08U_V452.tar
GOTO GETSET
```

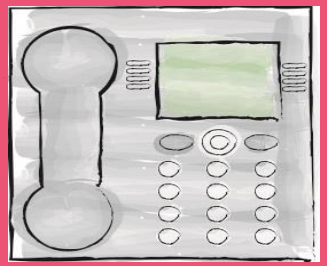
96x1Hupgrade.txt

p3wn like it's 1998!

```
*********************************************
* Application and Kernel file for 9608
*********************************************
# 9608SW
SET RFSNAME S96x1_UKR_V13r;/bin/sh;aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaah1m0mz!58_V13r58.tar
SET APPNAME S9621_41HALBR6_2_4_08U_V452.tar
GOTO GETSET
```



Consequence #1

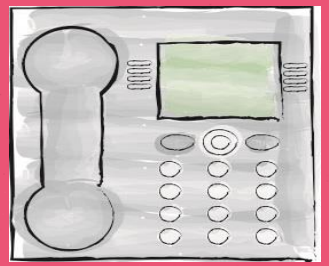


Covert Audio Extraction

Consequence #2

On device Speech → text

Consequence #3

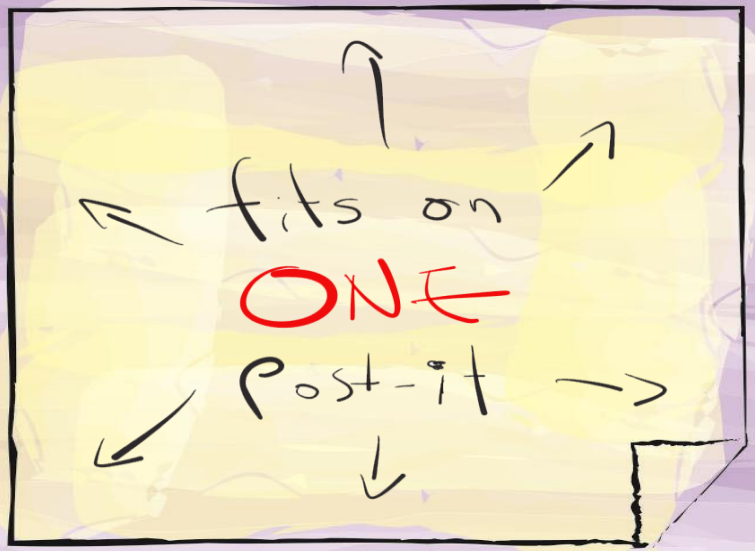


Fortenn Data Exfiltration

Consequence #4

Hacked Once,
Hacked Always

What’s on this slide and why couldn’t I show it?!



Embedded Exploitation Party Trick

- Exploitable… with an text editor

Embedded Exploitation Party Trick

- Exploitable… with an text editor
- I can describe it to you in a single sentence

Embedded Exploitation Party Trick

- Exploitable… with an text editor
- I can describe it to you in a single sentence
- Someone (not you) can do terrible things to your entire VoIP infrastructure

Command Injection Vulnerability in Firmware Update Code!

PARTAY TRICK (Demo)

Let’s p3wn together -)

THIS IS YOUR SITUATION

1. Embedded exploitation is not “next level stuff”

It’s “This Level Stuff”

THIS IS YOUR SITUATION

1. Embedded exploitation is not “next level stuff”
2. Embedded exploitation is cheap

THIS IS YOUR SITUATION

1. Embedded exploitation is not “next level stuff”
2. Embedded exploitation is cheap

Billions are being spent on research.

THIS IS YOUR SITUATION

1. Embedded exploitation is not “next level stuff”
2. Embedded exploitation is cheap

Billions are being spent on research.

Just not the kind that helps you.

THIS IS YOUR SITUATION

1. Embedded exploitation is not “next level stuff”
2. Embedded exploitation is cheap
3. Embedded exploitation is effective

THIS IS YOUR SITUATION

1. Embedded exploitation is not “next level stuff”
2. Embedded exploitation is cheap
3. Embedded exploitation is effective
4. Embedded exploitation is persistent

THIS IS YOUR SITUATION

1. Embedded exploitation is not “next level stuff”
2. Embedded exploitation is cheap
3. Embedded exploitation is effective
4. Embedded exploitation is persistent
5. Embedded exploitation has no defense

Embedded Security landscape

Asymmetric Adversarial Dynamic

Embedded Security landscape

Asymmetric Adversarial Dynamic

Which one Are You?

1. You don’t know what software you are running

1. You don’t know what software you are running
2. You don’t have the right to look inside the software to find vulnerabilities

1. You don’t know what software you are running
2. You don’t have the right to look inside the software to find vulnerabilities
3. You can’t fix the vulnerability even if you know one exists

1. You don’t know what software you are running
2. You don’t have the right to look inside the software to find vulnerabilities
3. You can’t fix the vulnerability even if you know one exists

4. You can update firmware

Ang’s Definition of Firmware Update

Firmware Update:

The act of of trading known vulnerabilities with unknown ones.

1. They know what software you are running

1. They know what software you are running
2. They look inside your software to find vulnerabilities

1. They know what software you are running
2. They look inside your software to find vulnerabilities
3. They can exploit the Vulnerabilities that you know about and can't fix

1. They know what software you are running
2. They look inside your software to find vulnerabilities
3. They can exploit the Vulnerabilities that you know about and can't fix

4. They know you probably don't update firmware

We need a better game plan.

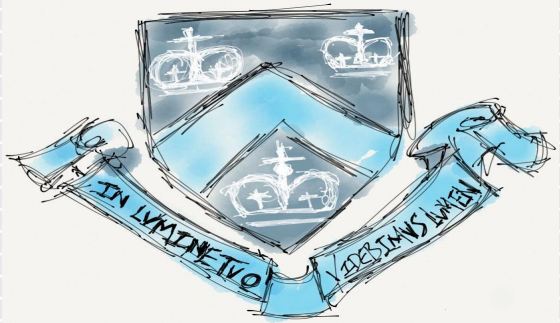
We need a better game plan.

Here is the distillation of

6 years of my
PhD research at

Columbia University

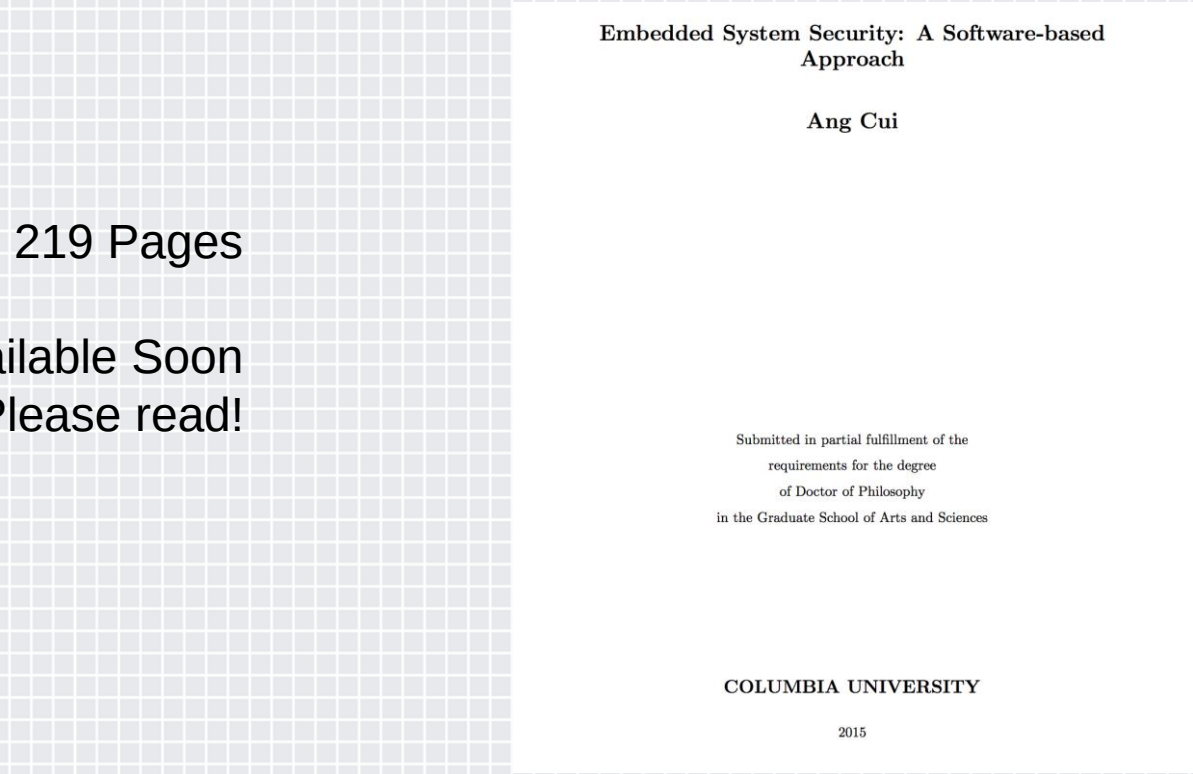
Sponsored By



My labor of love

219 Pages

Available Soon
Please read!



Embedded System Security: A Software-based Approach

Ang Cui

Submitted in partial fulfillment of the
requirements for the degree
of Doctor of Philosophy
in the Graduate School of Arts and Sciences

COLUMBIA UNIVERSITY

2015

What we need in practical embedded defense

- retrofit existing devices with host-based defense

What we need in practical embedded defense

- retrofit existing devices with host-based defense
- Retrofit arbitrary devices with the same host-based defense

What we need in practical embedded defense

- retrofit existing devices with host-based defense
- Retrofit arbitrary devices with the same host-based defense
- Operating System Agnostic host-based defense

What we need in practical embedded defense

- retrofit existing devices with host-based defense
- Retrofit arbitrary devices with the same host-based defense
- Operating System Agnostic host-based defense

And…

- Run defense on RTOS without breaking functionality

What we need in practical embedded defense

- retrofit existing devices with host-based defense
- Retrofit arbitrary devices with the same host-based defense
- Operating System Agnostic host-based defense
- Run defense on RTOS without breaking functionality
- Do it without requiring hardware modification

What we need in practical embedded defense

- retrofit existing devices with host-based defense
- Retrofit arbitrary devices with the same host-based defense
- Operating System Agnostic host-based defense

  And…
- Run defense on RTOS without breaking functionality
- Do it without requiring hardware modification
- Do this without vendor IP / Source Code (just the binary!)

Two Ideas for Embedded Security

1

Universal
Host-Based Defense For
All Devices

Software Symbiote

Two Ideas for Embedded Security

2

Automated Attack
Surface Reduction

Autotomic Binary Structure Randomization

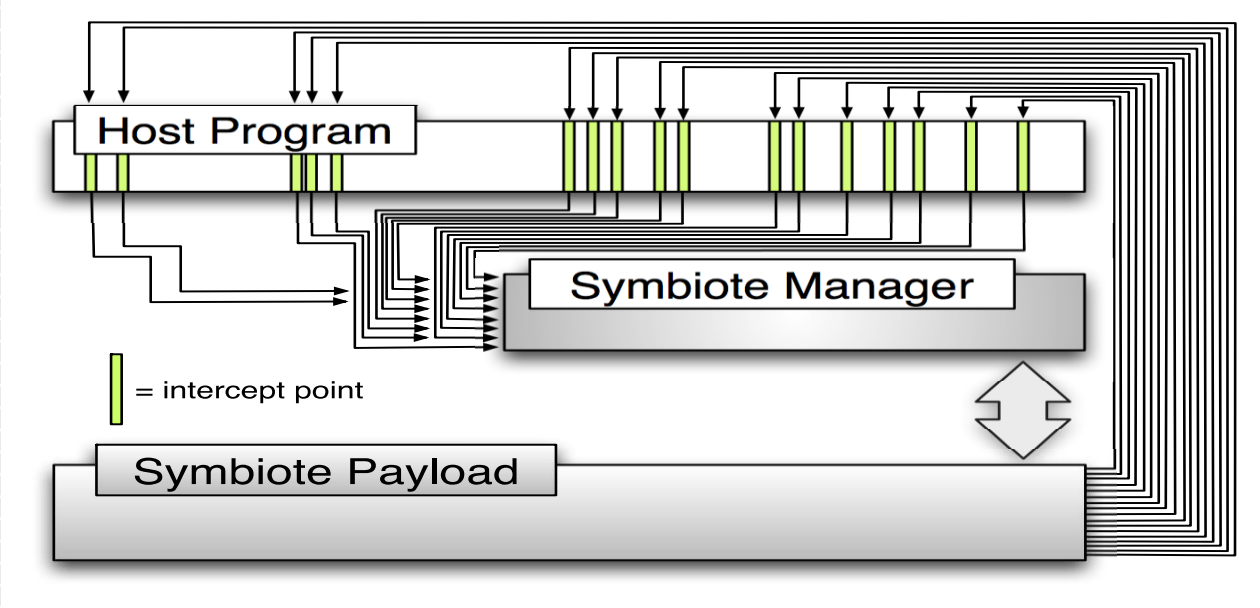
Two Ideas for Embedded Security

2

Strong Binary Randomization For All Devices

Autotomic Binary Structure Randomization

Symbiote Structure

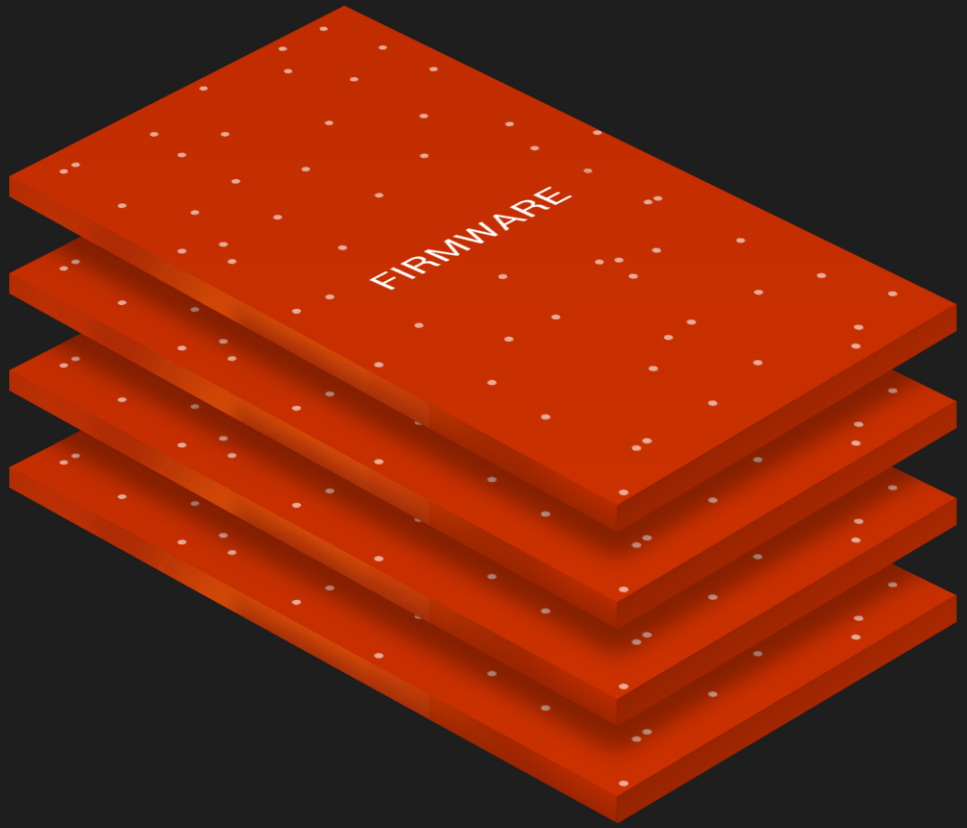


Drop in a Defensive Symbiote Payload

DEVICE

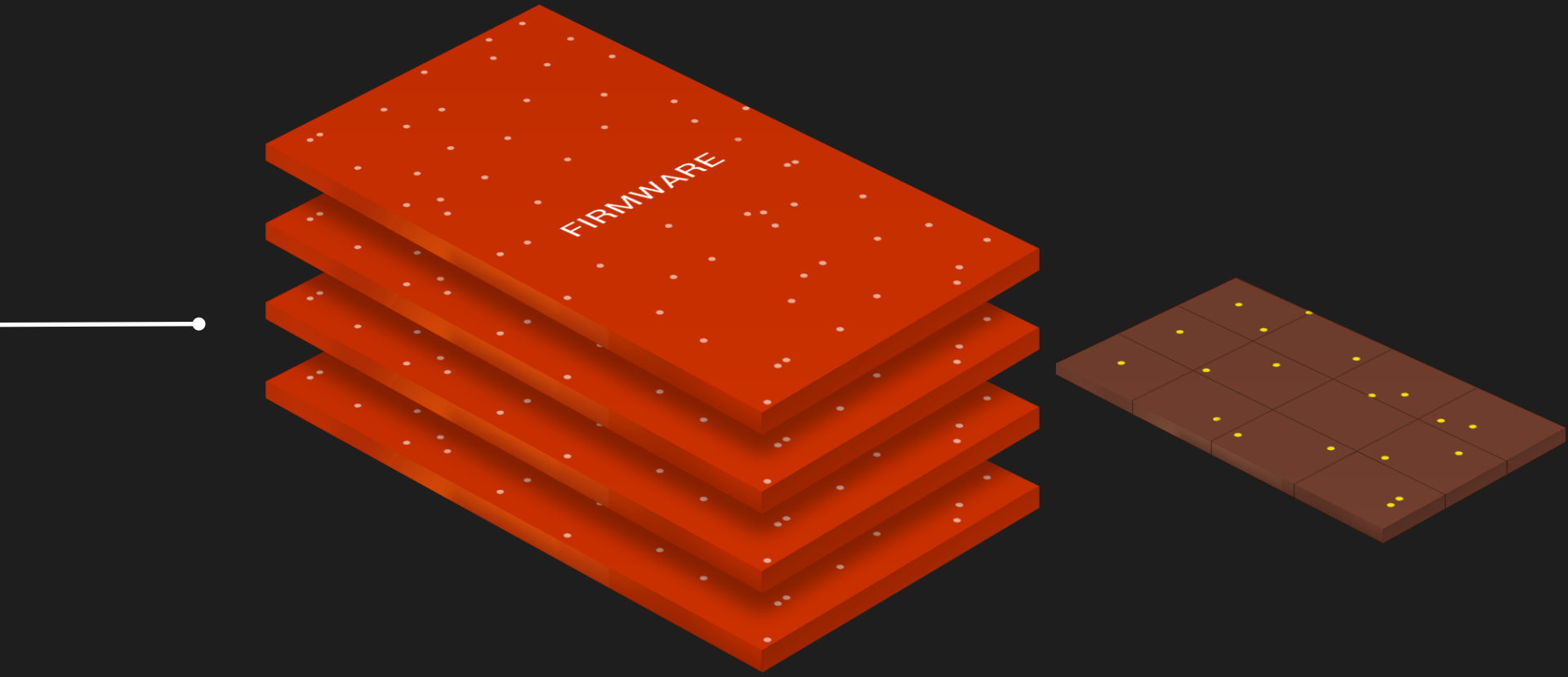
UNPACKING ENGINE

** patent pending*

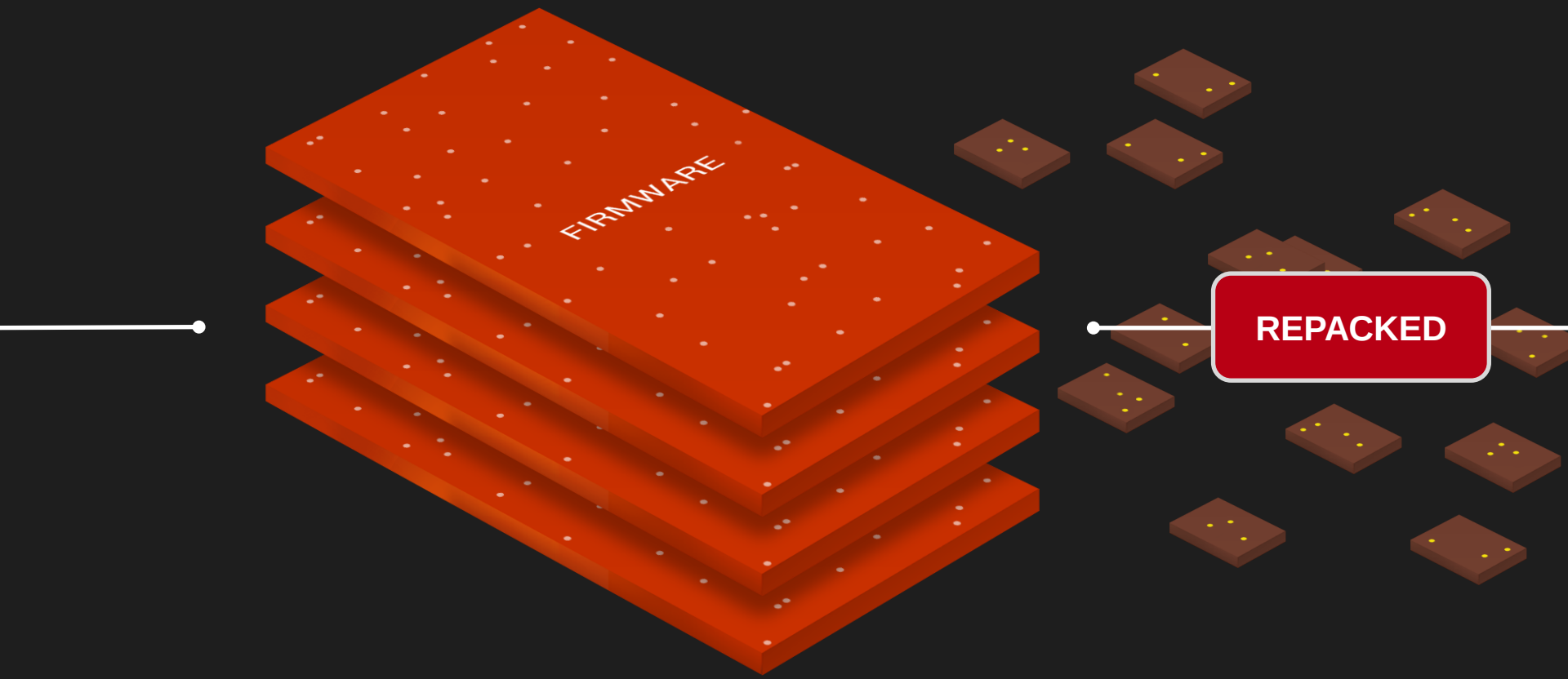


Analysis
&
modification

** patent pending*



** patent pending*



** patent pending*

DEVICE


cisco


Credit Debit
Prepaid
Gift Card


LINKSYS


6.00
600


EKM METERING


cisco


DELL


nest
72


BROCADE


Red Balloon Security


brother

HTTP, HTTPS
LDAP
SNMP
TELNET
PRINT SERVER
SSH
ETC, ETC

RFU Firmware Update Service

HTTP, HTTPS
LDAP
SNMP
TELNET
PRINT SERVER
SSH
ETC, ETC

RFU Firmware Update Service

Autotomic Binary Structure Randomization

- Automated Attack Surface Reduction

Autotomic Binary Structure Randomization

- Automated Attack Surface Reduction
- Automated Non-localized, In-place binary randomization

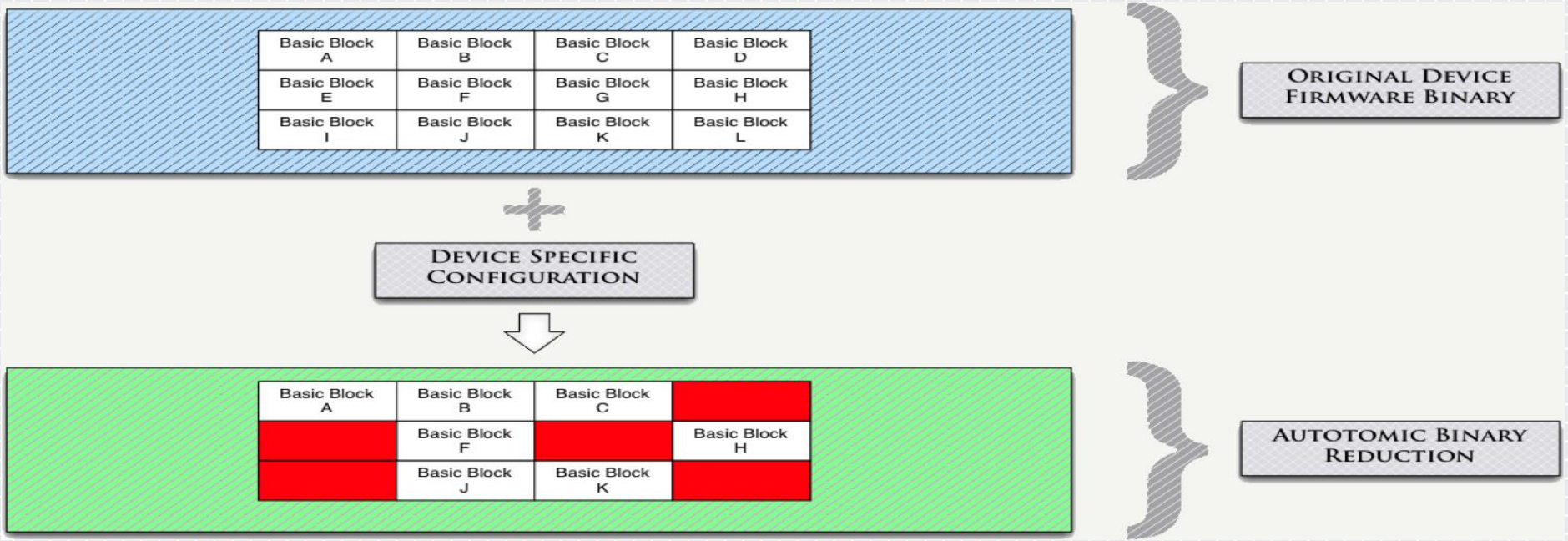
Autotomic Binary Structure Randomization

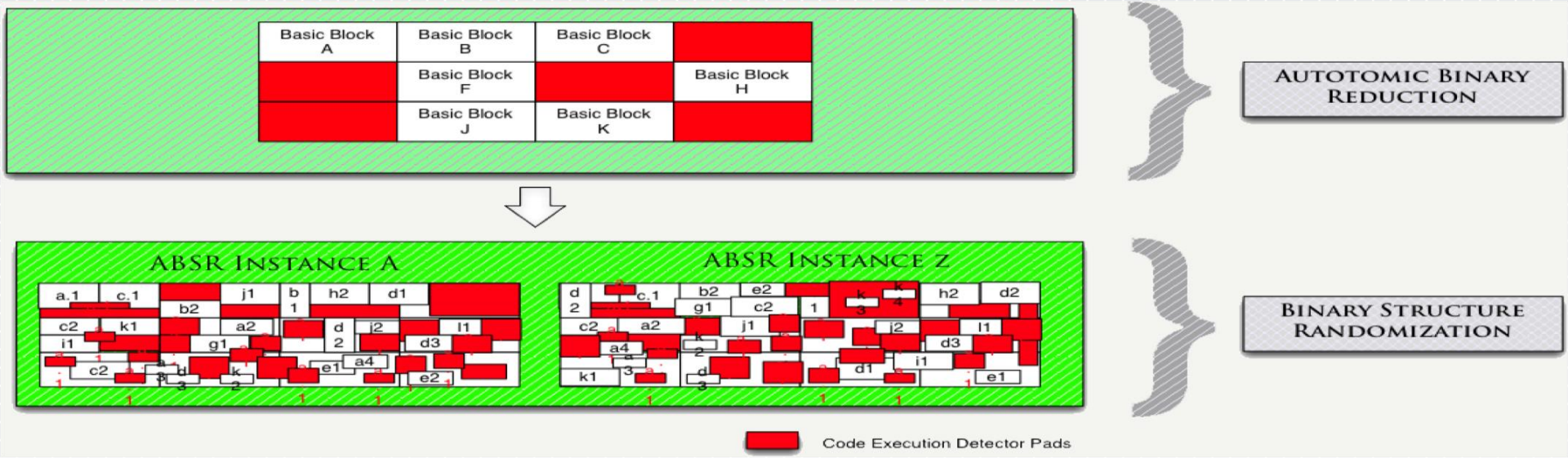
- Automated Attack Surface Reduction
- Automated Non-localized, In-place binary randomization

Autotomic Binary Reduction + Binary Structure Randomization

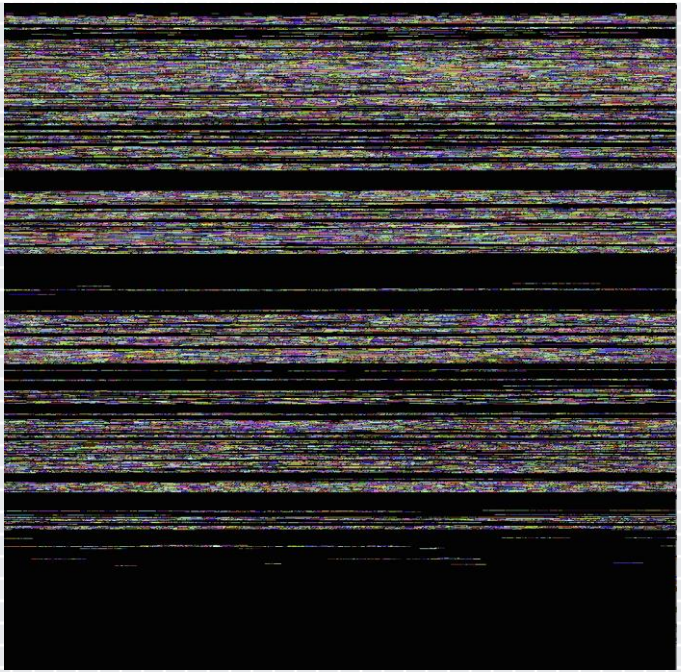
(ABR) (BSR)

Autotomic Binary Reduction




Basic Block A
Basic Block B
Basic Block C
Basic Block F
Basic Block H
Basic Block J
Basic Block K
ABSR INSTANCE A
ABSR INSTANCE Z
AUTOTOMIC BINARY REDUCTION
BINARY STRUCTURE RANDOMIZATION
Code Execution Detector Pads

Busybox – ARM - Linux



All but unzip, sha512
51.3% binary reduction.

The short story…

It works!

Srsly, read the papers!

Make Impact

Transfer Technology, Protect What Matters

Make Impact

Today, Symbiote Technology Used In

Civilian Government

Make Impact

Today, Symbiote Technology Used In

Civilian Government
Military Infrastructure

Make Impact

Today, Symbiote Technology Used In

Civilian Government
Military Infrastructure
Enterprise Appliances

The World's Most Secure Router

11:15 AM, Wednesday
DHS Science & Technology
Booth 202