

# Security Basics

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	User Authentication Trends and Methods for Native Mobile Applications	Kayvan Alikhani
10:15 AM	BREAK	
10:30 AM	Mobile & IOT Security: Will Big Data Make it Better or Worse?	Hadi Nahari
11:15 AM	Viruses, Malware and Threats	Tas Giakouminakis
12:00 PM	LUNCH	
1:15 PM	Crypto 101: Encryption, Codebreaking, SSL, and Bitcoin	Benjamin Jun
2:00 PM	Security Enforcement Explained	Dana Wolf
2:45 PM	BREAK	
3:00 PM	Internet and Web Security Issues	Patrick Sullivan
3:45 PM	Network Security	Gary Sockrider

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SEM-M01

## Introduction and A Look at Security Trends

Hugh Thompson, Ph.D.

---

Program Committee Chairman, RSA Conference  
Twitter: @DrHughThompson

# CHANGE

Challenge today's security thinking



# WELCOME TO THE PADANGTEGAL MANDALA WISATA WANARA WANA SACRED MONKEY FOREST SANCTUARY

DEAR VISITORS,

ON BEHALF OF THE VILLAGE OF PADANGTEGAL AND THE WANARA WANA FOUNDATION WE WISH YOU AN ENJOYABLE AND EDUCATIVE VISIT TO OUR FOREST SANCTUARY AND TEMPLE COMPLEX. TO ENSURE A TRULY PLEASANT VISIT PLEASE OBSERVE THE FOLLOWING:

1. THIS IS A SACRED AREA. PLEASE COMPORT YOURSELF WITH RESPECT FOR THE PEOPLE WHO WORSHIP HERE, THE TEMPLES AND THE MONKEYS AND OTHER PLANTS AND ANIMALS THAT RESIDE IN THE FOREST.
2. THE MONKEYS OF THIS FOREST ("KERA" OR "MURAKOK") ARE FREE LIVING WILD MAMMALS. PLEASE REFRAIN FROM TOUCHING OR PLAYING WITH THEM AS THEY MAY REACT IN AN UNPREDICTABLE MANNER. DO NOT PROVIDE FENNELS FOR THE MONKEYS AS THEY ARE A POTENTIAL HEALTH RISK. SEEK OUT A STAFF MEMBER (GREEN SHROUD) FOR ANY ASSISTANCE REGARDING THE MONKEYS.
3. PLEASE READ THE BROCHURE PROVIDED WITH THE ENTRANCE TICKET FOR FURTHER INFORMATION ABOUT THIS SANCTUARY.

WE THANK YOU FOR FOLLOWING THESE REQUIREMENTS AND WE TRUST THAT YOUR VISIT WILL BE A MEMORABLE ONE.

SINCERELY,  
WANARA WANA FOUNDATION



# Agenda

Intro to Information Security

Economics of Information Security

Security Trends



# The Shifting IT Environment

(...or why security has become so important)

# Shift: Compliance and Consequences

- ◆ The business has to adhere to regulations, guidelines, standards,...
  - ◆ SAS 112 and SOX (U.S.) – upped the ante on financial audits (and supporting IT systems)
  - ◆ PCI DSS – requirements on companies that process payment cards
  - ◆ HIPAA, GLBA, BASEL II, ..., many more
- ◆ Audits have changed the economics of risk and create an “impending event”

**Hackers *may* attack you but auditors *will* show up**

- ◆ Disclosure laws mean that the consequences of failure have increased
  - ◆ Waves of disclosure legislation

# Shift: Technology

- Many applications/transactions now operate over the web
- Cloud is changing our notion of a perimeter
- Worker mobility is redefining the IT landscape
- Shadow IT is becoming enterprise IT
- Majority of web transactions are now encrypted (SSL)
- The security model has changed from good people vs. bad people to enabling partial trust
  - There are more “levels” of access: Extranets, partner access, customer access, identity management, ...



# Shift: Attackers

- ◆ Cyber criminals are becoming organized and profit-driven
  - ◆ An entire underground economy exists to support cybercrime
- ◆ Attackers are shifting their methods to exploit both technical and human weaknesses
- ◆ Attackers after much more than traditional monetizable data (PII, etc.)
  - ◆ Hacktivism
  - ◆ State-sponsored attacks
  - ◆ IP attacks/breaches



# Shift: Customer expectations

- ◆ Customers, especially businesses, are using security as a discriminator
- ◆ In many ways security has become a non-negotiable expectation of businesses
- ◆ Security being woven into service level agreements (SLAs)
- ◆ The “average person” is now familiar with security



# Big Questions

- ◆ How do you communicate the value of security to the enterprise (and management)?
- ◆ How do you measure security?
- ◆ How do you rank risks?
- ◆ How do you reconcile security and compliance?
- ◆ How can you be proactive and not reactive? What is “security intelligence” and how would you actually consume, act on or share it?
- ◆ What changes are likely in privacy laws, data sovereignty, trust?
- ◆ What about big issues in the news like APT’s, hacktivism, leaks, DDoS attacks, ...? How should/can we adapt what we do based on them?
- ◆ How do you adapt to new paradigms like IoT?

# The Economics of Security

## Hackernomics (*noun*)

A social science concerned chiefly with description and analysis of attacker motivations, economics, and business risk. Characterized by

**5 fundamental immutable laws and 4 corollaries**



# Law 1

Most attackers aren't evil or insane; they just want something

Corollary 1.a.:

We don't have the budget to protect against evil people but we *can* protect against people that will look for weaker targets



## Law 2

Security isn't about security. It's about mitigating risk at some cost.

Corollary 2.a.:

In the absence of metrics, we tend to over focus on risks that are either familiar or recent.

## Law 3

Most costly breaches come from simple failures, not from attacker ingenuity

Corollary 3.a.:

Bad guys can, however, be VERY creative if properly incentivized.

# The CAPTCHA Dilemma

Completely

Automated

Public

Turing test to tell

Computers and

Humans

Apart

*following*

*finding*

*sim~m*



## Law 4

In the absence of security education or experience, people (employees, users, customers, ...) naturally make poor security decisions with technology

Corollary 4.a.:

Systems needs to be **easy to use securely and difficult to use insecurely**





## Law 5

Attackers usually don't get in by cracking some impenetrable security control, they look for weak points like trusting employees



# A Visual Journey of Security Trends

**2008**







# Enjoy the rest of the conference!!

# Security Basics

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	User Authentication Trends and Methods for Native Mobile Applications	Kayvan Alikhani
10:15 AM	BREAK	
10:30 AM	Mobile & IOT Security: Will Big Data Make it Better or Worse?	Hadi Nahari
11:15 AM	Viruses, Malware and Threats	Tas Giakouminakis
12:00 PM	LUNCH	
1:15 PM	Crypto 101: Encryption, Codebreaking, SSL, and Bitcoin	Benjamin Jun
2:00 PM	Security Enforcement Explained	Dana Wolf
2:45 PM	BREAK	
3:00 PM	Internet and Web Security Issues	Patrick Sullivan
3:45 PM	Network Security	Gary Sockrider

SESSION ID: SEM-M01

## User Authentication Trends and Methods for Native Mobile Applications

Kayvan Alikhani

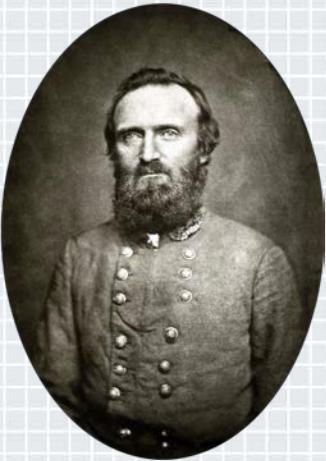
Senior Director of Technology  
RSA

# CHANGE

Challenge today's security thinking



# Authenticate: Prove you are who you claim to be



Stonewall Jackson

...A Union cavalry force shouted "Halt, who goes there?", but fired before evaluating the reply. Frantic shouts by Stonewall Jackson's staff identifying the party were replied to:

"It's a damned Yankee trick! **Fire!**"

Jackson was severely wounded & ended up dying of the gun wound.

## Worst. Authentication. Ever?

Did they use a Pass phrase?

If not, was it the environment that failed them?

Too Loud to recognize his voice? Too dark to identify him?

Or a simple case of Timeout!

# Strong Auth



- ◆ **Strong Authentication** The requirement to use **multiple factors** for authentication... to verify an entity's identity

*(National Information Assurance (IA) Glossary)*



# Strong Auth: Multi-factor vs. Multi-layered

- ◆ **Multi-factor** auth: Authentication that requires the use of solutions from two or more of categories of factors
- ◆ **Multi-layered** auth: Using multiple solutions from varying (same/different) categories at different **points** in the process

# Biometric Auth: Fingerprinting: 'Old' school method

200 BC:  
China



Handprints used  
as evidence for  
burglaries

1892:  
UK



Galton:  
"Fingerprints":  
Individuality &  
permanence,  
introduced 'minutia'

1915:  
Oakland



International  
Association for  
Criminal  
Identification

2015:  
Everywhere



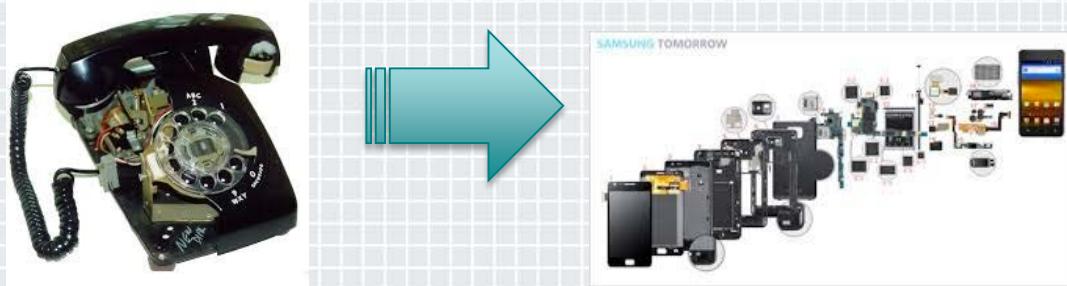
# Other Biometric auth methods for mobile apps

- ◆ Voice print
- ◆ Face print (including eye veins)
- ◆ Iris
- ◆ EKG: Heart-signature
- ◆ Behavioral patterns
- ◆ Ear pattern (no, this is not a typo)
- ◆ ....



# Biometric auth: The Mobile advantage

- ◆ Modern devices now equipped with powerful sensors & radios:
  - ◆ Camera(s)
  - ◆ Microphone(s)
  - ◆ Fingerprint sensor
  - ◆ GPS/Wi-Fi/Bluetooth
  - ◆ Gyro/Accelerometer
  - ◆ IR Laser/LED
- ◆ Plus...We carry them everywhere!



# Mobile biometrics for mobile apps: What to Watch Out For!

- ◆ Has to be easy for the user, as in: “Work all the time!” for the right user:
  - ◆ Tolerable False Acceptance & Rejection rates
  - ◆ Adapts to Environment: Too loud, Too dark, Too cold? No problem!
  - ◆ Matches user/organizational needs: Compliant
- ◆ Protect Data at rest:
  - ◆ Securely stores & protects sensitive data: Templates/hashes/keys
  - ◆ Takes advantage of hardware security when possible
- ◆ Protect Data being acquired:
  - ◆ Live-ness detection: Prevent spoofing



# Mobile Auth trends and standards

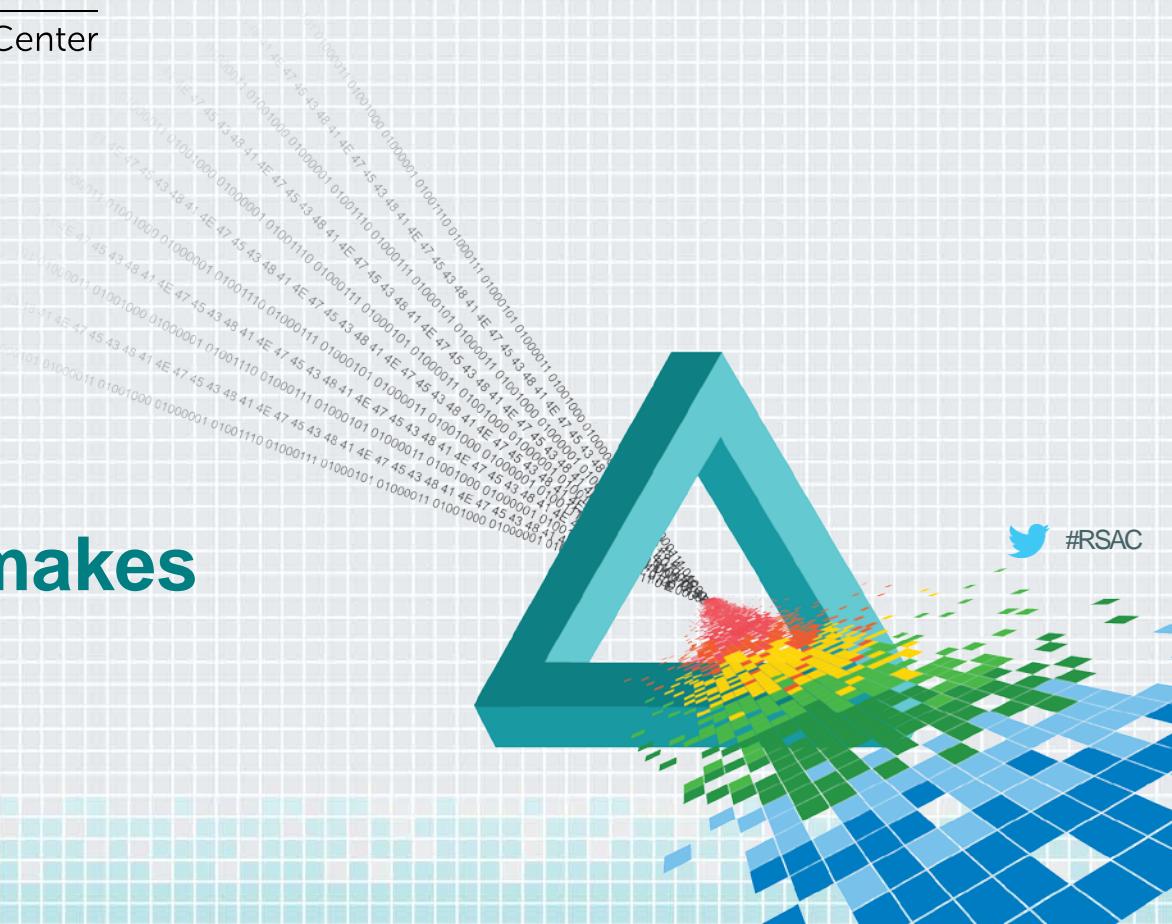
- ◆ FIDO Alliance, Apple Touch ID, Windows 10 (TPM):
  - ◆ Auth on the device: Move from server based Auth to device-side Auth
  - ◆ Credentials/Biometric templates never leave the device
  - ◆ Device “signs” claims and assertions
- ◆ Use of HW to protect keys/processes:
  - ◆ Use of TEE, SE to store key data at rest
  - ◆ Use of TEE to run authentication process



# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

## Multi-factor Auth makes sense!



# Reality vs. Utopia

## ◆ **Utopia:**

- ◆ Devices: All have well designed, easy to use, similar authenticators
- ◆ Service providers: All support a common standard for authentication
- ◆ Hackers: Leave device-side biometric authentication “alone”

## ◆ **Reality (for the next ~5 years):**

- ◆ Devices: Growing mix of different capabilities, makes & models
- ◆ Service providers: Hodgepodge of Auth protocols and standards
- ◆ Hackers: Can't wait...



# Dos and Don'ts for mobile app auth solutions

- ◆ Don't put all your eggs in one basket, throw a wider net:
  - ◆ Design around solutions that take advantage of **evolving** mobile auth methods
  - ◆ **Avoid** solely relying on a single:
    - ◆ Factor/Method
    - ◆ Vendor
    - ◆ Platform/OS
  - ◆ Look for standards support and compliance
- ◆ Determine Risk:
  - ◆ Take advantage of solutions that include "**User behavioral data**" to make better decisions. Data that includes:
    - ◆ User location, network, device registration, usage and activity pattern



# Dos and Don'ts for mobile app auth solutions

- ◆ Survey your users with simple POCs to see what method ‘works’ for them
- ◆ Remember: Combining auth methods **lowers** the risk of each method:
  - ◆ Improves chance of information being accessed by the right person
- ◆ It's a Balancing Act:
  - ◆ Decide when to use “step up” based on “role” & “action”, for example:
    - ◆ User is reviewing NBA game stats? Let them in, accept **Moderate risk**
    - ◆ Manager is Approving a players transfer? Step up & tolerate **Lower risk**

# Security Basics

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	User Authentication Trends and Methods for Native Mobile Applications	Kayvan Alikhani
10:15 AM	BREAK	
10:30 AM	Mobile & IOT Security: Will Big Data Make it Better or Worse?	Hadi Nahari
11:15 AM	Viruses, Malware and Threats	Tas Giakouminakis
12:00 PM	LUNCH	
1:15 PM	Crypto 101: Encryption, Codebreaking, SSL, and Bitcoin	Benjamin Jun
2:00 PM	Security Enforcement Explained	Dana Wolf
2:45 PM	BREAK	
3:00 PM	Internet and Web Security Issues	Patrick Sullivan
3:45 PM	Network Security	Gary Sockrider

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SEM-M01

## Mobile & IoT Security: Will Big Data Make it Better or Worse?

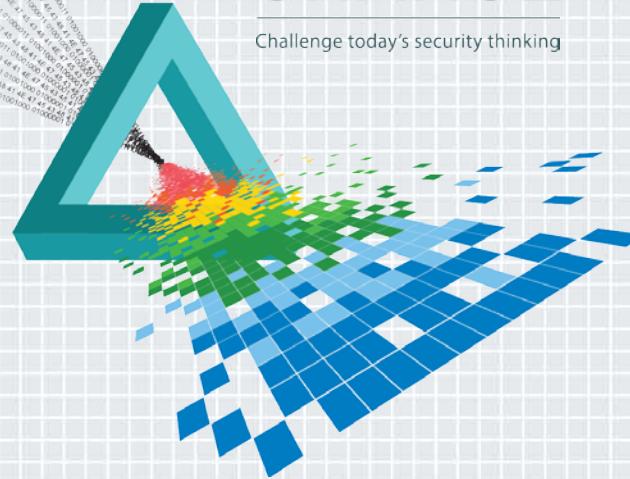
Hadi Nahari

---

Chief Security Architect  
NVIDIA  
@hadinahari

# CHANGE

Challenge today's security thinking



# Threat Landscape

>3,000,000,000,000

threats annually

legacy threats

blocked

advanced threats

detected

undetected

50%

25%

25%

1.6 B

number of records lost globally in 2014

\$236 M

recovery cost of Target breach (so far)

15 B

connected devices in 2015

(avg. \$27.3 loss per incident)

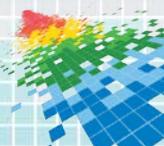
\$110 BN

the annual price tag  
of cybercrime



# Motivation

- ◆ More connected devices → more value → added risk
- ◆ Security posture hasn't magically improved
  - ◆ In many cases in fact it has regressed
- ◆ Heterogeneous security paradigms
  - ◆ Device-end data is dislodged and processed separately
  - ◆ Dubious security posture of the Big Data infrastructure itself
  - ◆ Unclear how it handles the security of the data it analyzes
- ◆ A massive digital orgy with no reliable membranes



# Increasing Complexity

- ◆ Space Shuttle: ~400K LOC
- ◆ F22 Raptor fighter Jet: ~2M LOC
- ◆ Linux kernel 2.2: ~2.5M LOC
- ◆ Hubble Space Telescope: ~3M LOC
- ◆ Android Core: 12M LOC
- ◆ Future Combat System: 63M LOC
- ◆ Connected Car: 100M LOC
- ◆ Autonomous Vehicle: 300M LOC



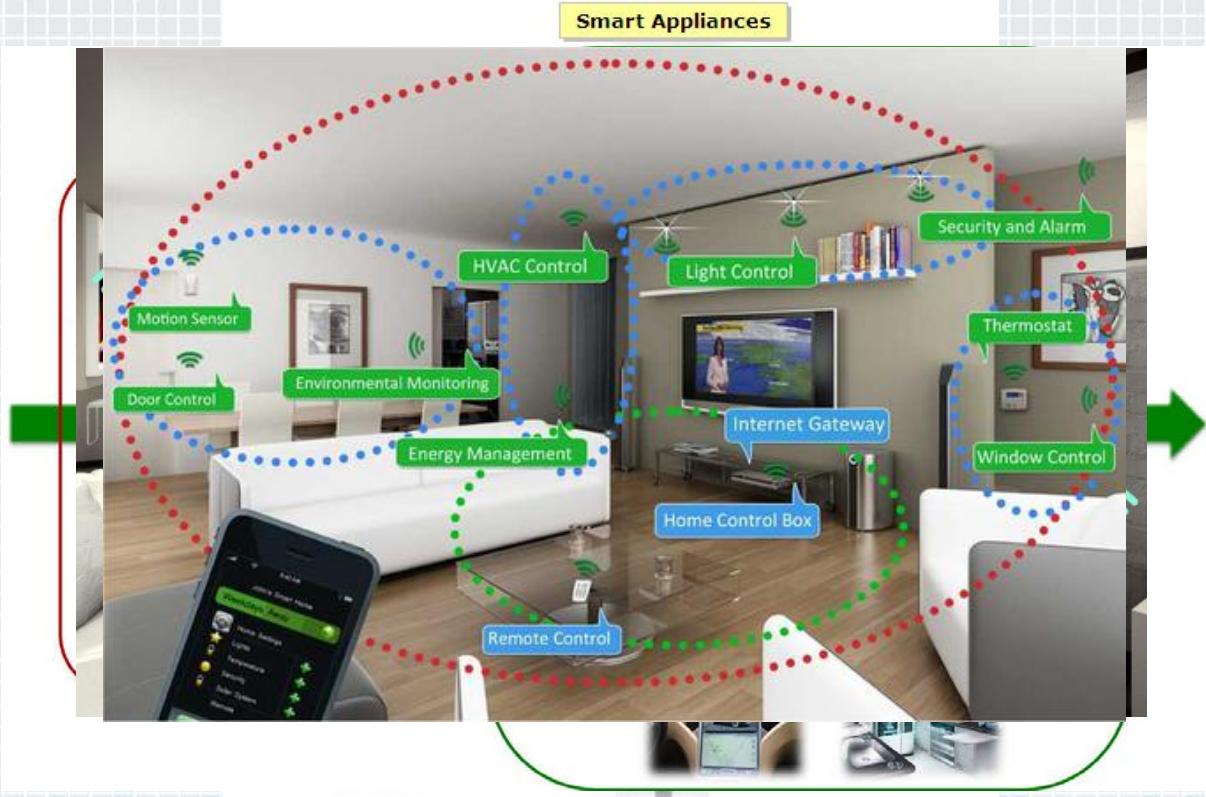
# Mobile



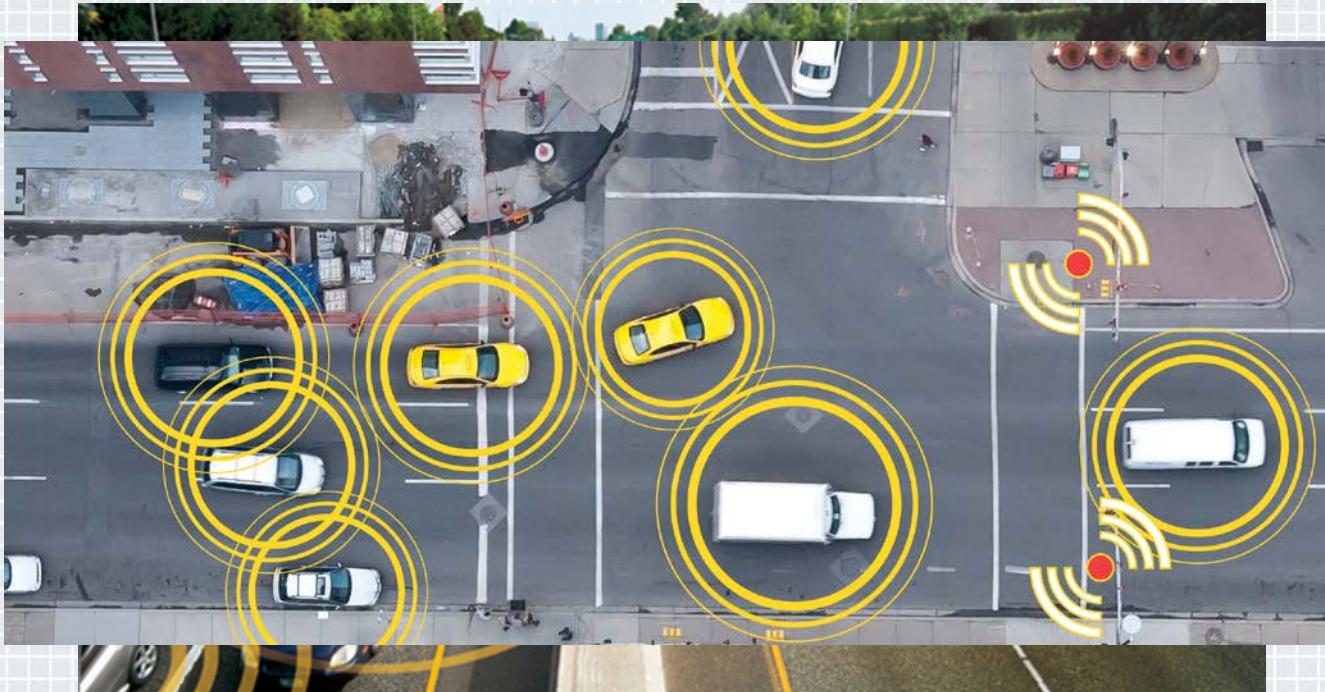
# Mobile Security

- ◆ Mobile security posture is (somewhat) stabilizing
- ◆ Core framework and device technologies finally maturing
  - ◆ ROT/COT, SEforAndroid, ARM TrustZone, Mobile TPM/HSM, e/SE, etc.
  - ◆ Foundation technologies have/are being commoditized
- ◆ Ecosystem(s) consolidating:
  - ◆ SoC, OEM/ODM, Stack/OS, MNO, SP, MDM
- ◆ Liability boundaries better understood now than in early days
- ◆ More capable (and cheaper) devices → more value-added services
- ◆ Mobile attack surface hardening → attackers go for softer targets

# IoT (Thingsternet)



# Vehicle: IoT?





# Incentives

- ◆ Known vulnerabilities (phone era) softer target (IoT)
  - ◆ ATO, escalation of privileges, ROT/COT, etc.
- ◆ Multi-device → multi-channel attack surface
- ◆ Counterfeit/black market: **\$45B/Y** market (magic box via OBD-II)
- ◆ Odometer rollback: **€6B/Y** in Germany
- ◆ Collect PII: vehicle as a soft entry
- ◆ Roughly **\$1T/Y** on a global basis
  - ◆ Potentially exceeding car crash, drug trafficking, and pilferage



© Ilya Genkin. [www.genkin.org](http://www.genkin.org)

## Connected Vehicle Security

# IoT Security

- ◆ Lack of standardized (or well-defined) orchestration layer
- ◆ Heterogeneous security capabilities
- ◆ Multi device management
  - ◆ Prone to TOCTU attacks, among others
- ◆ Dangerous “atomic” view of the IoT devices
  - ◆ False sense of security
- ◆ Technologies, usecases, actors, and attacks still evolving

# Big Data

“Big  
ever  
nol  
eve  
so  
*Data*



UNSTRUCTURED  
BIG DATA



I WANT YOUR  
DATA NOW



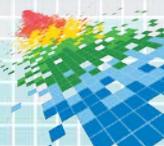
APPLY INSIGHTS

© DISCOVIX 2012



# Big Data Security

- ◆ Ok, what does it mean?
  - ◆ Cloud/infrastructure?
  - ◆ Comm. Channel?
  - ◆ Data (DAR/DIT)?
  - ◆ Stack (DAC/MAC)?
  - ◆ End point(s)?
- ◆ However you look
  - ◆ It's not fully new, but
  - ◆ It's not really secure either



# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

# Case Study: Identity Assertion & Authentication

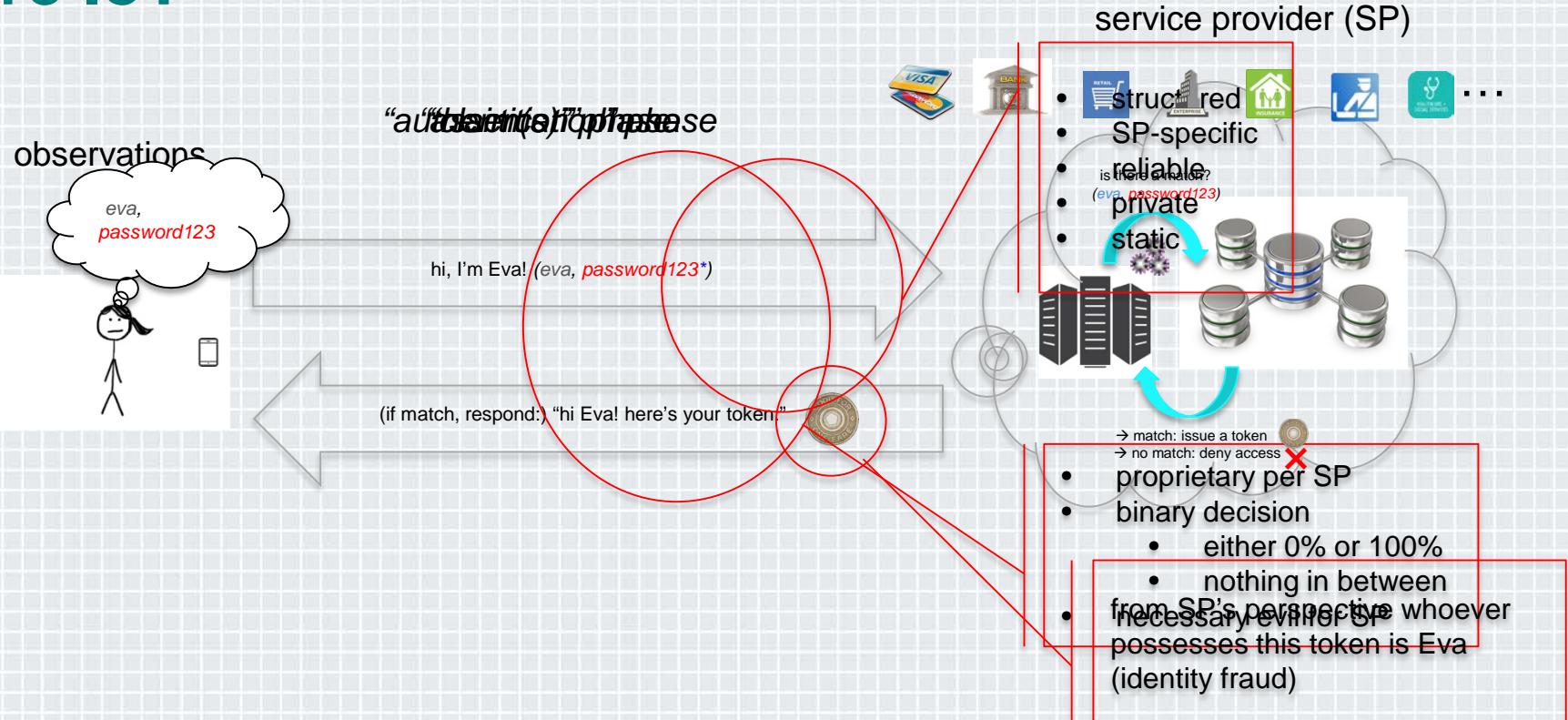




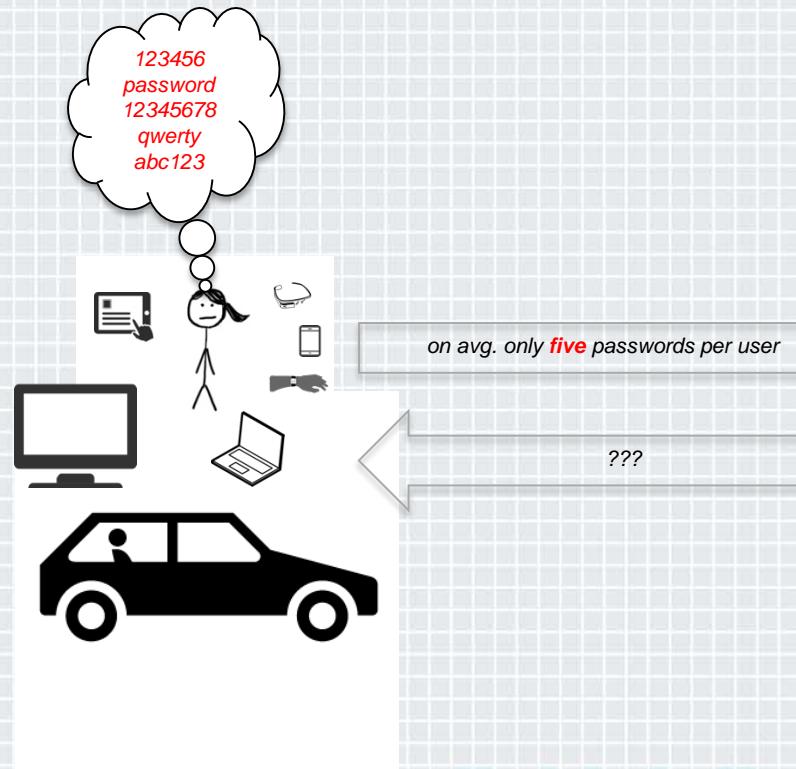
## Digital Identity Assertion Dilemma

*"On the Internet, nobody knows you're a dog" –Peter Steiner*

# Pre IoT



# IoT Era



# Results

Breach count by victim industry and employee count\*

1 to 100	1	2	10	1	79	5	18	14	3	1	3	3	38	6	2	7	193										
101 to 1,000			13	3	1	8	3		5	1	2	1	13	2	4	1	57										
1,001 to 10,000		1	7	1	3	22	10	12	6	1	2	1	2	1	2		71										
10,001 to 100,000		2	13	1	4		2	93	5			1		1		1	122										
More than 100,000	1	4		2			31		1			2	1	2	5	23	42										
Unknown			1	7	1	14	73	1	5	1		1	2	2	5	31	136										
Total	2	7	2	46	3	96	24	39	230	1	36	6	5	6	14	31	621										
					Agriculture (11)	Mining (21)	Utilities (22)	Construction (23)	Manufacturing (31)	Wholesale Trade (42)	Retail (44)	Transportation (48)	Information (51)	Finance (52)	Real Estate (53)	Professional (54)	Management (55)	Administrative (56)	Educational (61)	Healthcare (62)	Recreation (71)	Accommodation (721)	Food Services (722)	Other Services (81)	Public (92)	Unknown	Total

\* Industries based on [NAICS](#)

some noteworthy breaches since this report was released



TARGET



CK systems  
omni-channel retail solutions

iTunes

59

SEARS

JPMorganChase



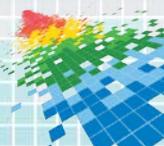
Anthem



RSA Conference 2015

# Conclusion/Apply

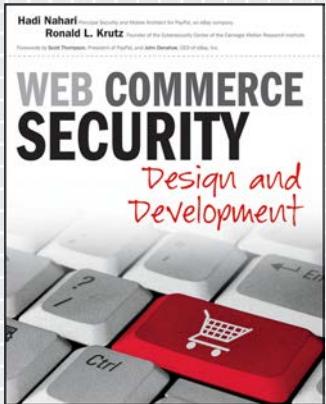
- ◆ IoT without Big Data be like FB without friends...
- ◆ IoT + Big Data: potentially less secure than either one alone
- ◆ IoT attacks ~~are becoming~~ have already become scalable
  - ◆ If your security solution is not real-time, you'll play catch
  - ◆ Attackers will have advantage for sometime
- ◆ Getting distributed security right is hard
- ◆ Getting data protection in heterogeneous environment is harder
- ◆ Increased threats → priority attention → scalable solutions



# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

# Thank You!



Hadi Nahari  
[hnhahari@nvidia.com](mailto:hnhahari@nvidia.com)  
  hadinahari



# Security Basics

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	User Authentication Trends and Methods for Native Mobile Applications	Kayvan Alikhani
10:15 AM	BREAK	
10:30 AM	Mobile & IOT Security: Will Big Data Make it Better or Worse?	Hadi Nahari
11:15 AM	Viruses, Malware and Threats	Tas Giakouminakis
12:00 PM	LUNCH	
1:15 PM	Crypto 101: Encryption, Codebreaking, SSL, and Bitcoin	Benjamin Jun
2:00 PM	Security Enforcement Explained	Dana Wolf
2:45 PM	BREAK	
3:00 PM	Internet and Web Security Issues	Patrick Sullivan
3:45 PM	Network Security	Gary Sockrider

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SEM-M01

## Viruses, Malware and Threats

Tas Giakouminakis

---

Co-Founder and Chief Technology Officer  
Rapid7

# CHANGE

Challenge today's security thinking



# The Beginning

**1966**  
Theory of  
Self-  
Reproducing  
Automata



**1983**  
Virus term  
coined



**1988**  
Morris worm  
first Internet  
worm



**2000s**  
Internet  
spreading  
worms  
ILOVEYOU,  
Slammer,  
MyDoom,  
Netsky,  
botnets, ...



**1971**  
Creeper  
experimental  
worm on  
DEC PDP-  
10/TENEX

Reaper worm  
removes  
Creeper

**1986**  
Brain first  
IBM PC virus

**1990s**  
DOS &  
Windows  
viruses and  
worms

# The Evolution

**2007**  
Storm  
worm  
botnet



**2008**  
Conficker  
botnet



**2010**  
APT gains  
publicity,  
Stuxnet  
cyber  
weapon



**2011**  
Bit-coin  
mining  
malware  
begins to  
rise



**2014**  
Fileless  
malware &  
kits gain  
popularity



**2007**  
Zeus  
crimeware  
kit

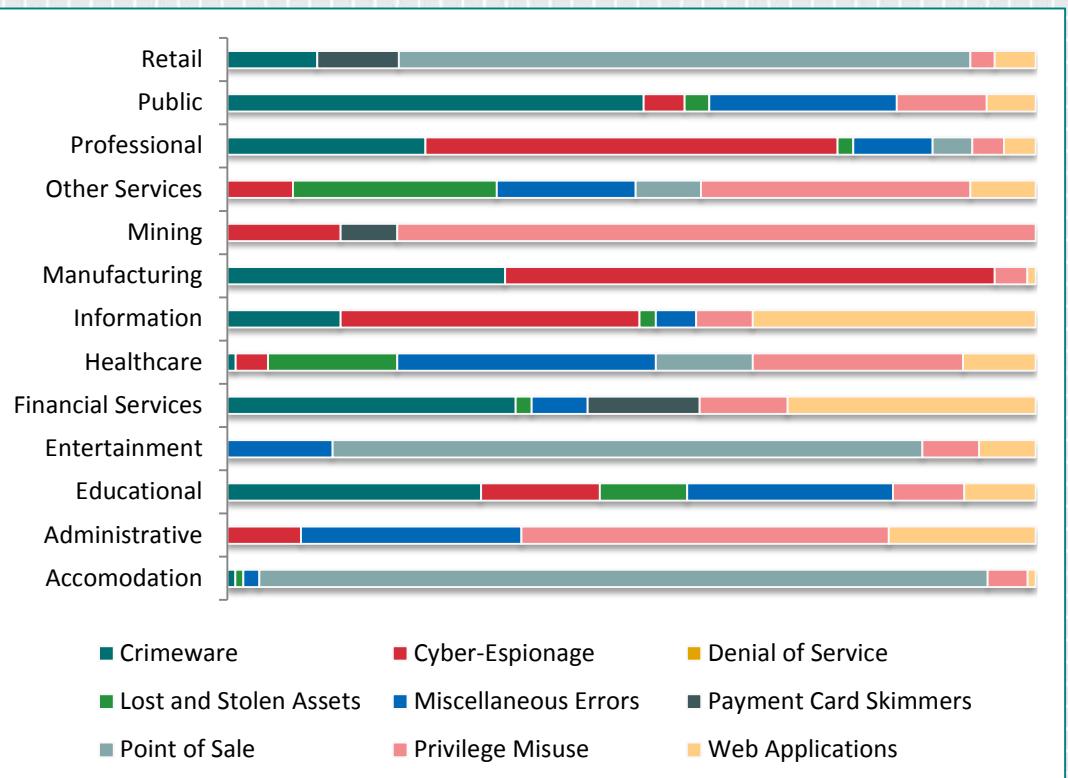
**2009**  
SpyEye

**2011**  
SpyEye &  
Zeus  
merge

**2012**  
Dexter  
Point-of-  
Sale botnet

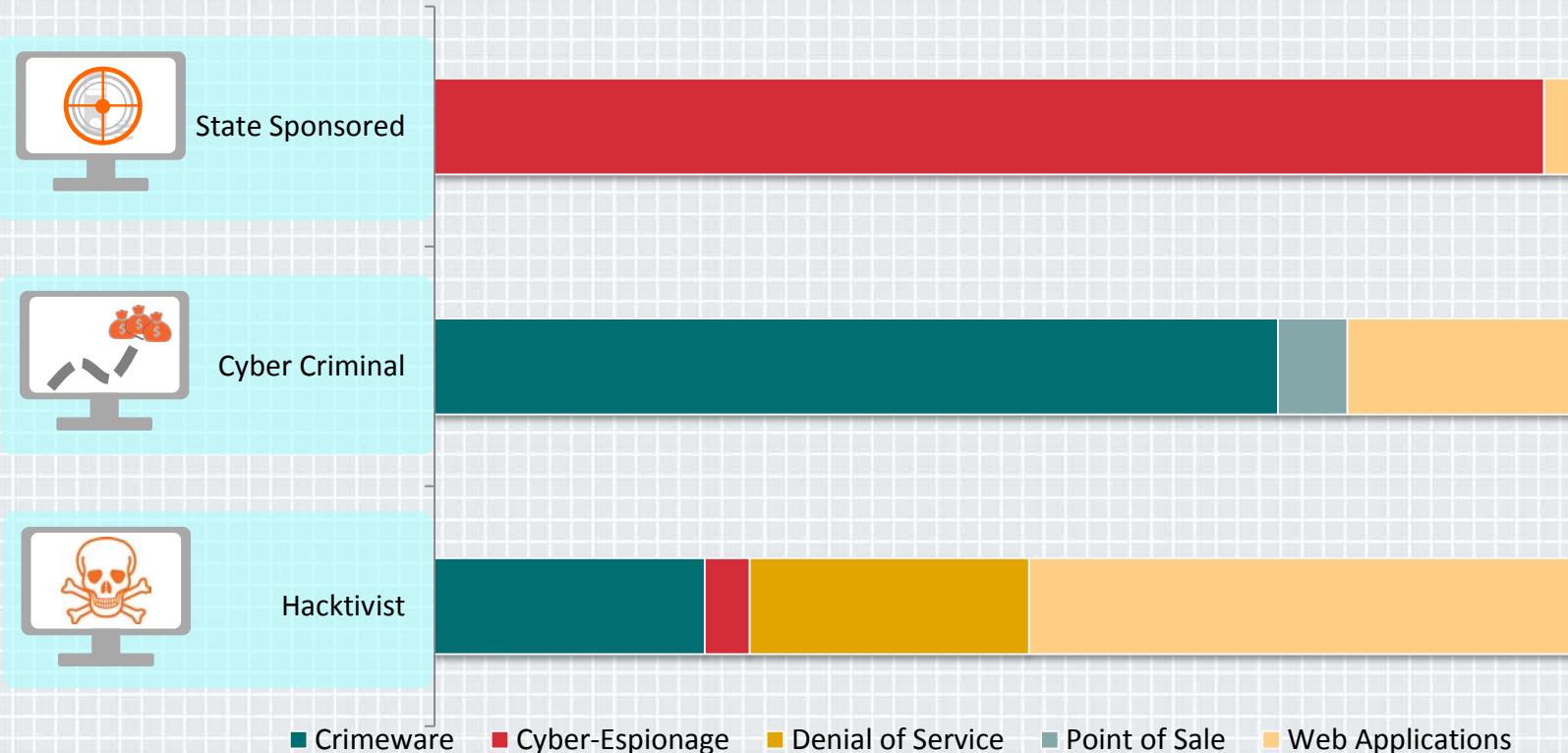
# Threats, threats, everywhere

- ◆ Common threats impact everyone
  - ◆ Mass malware
  - ◆ “Unintentional” insiders
- ◆ Gain insight into industry specific threats
  - ◆ ISACs
  - ◆ Public/Private initiatives
  - ◆ Vendors



Source: Verizon 2015 Data Breach Investigations Report

# Know Your Enemy

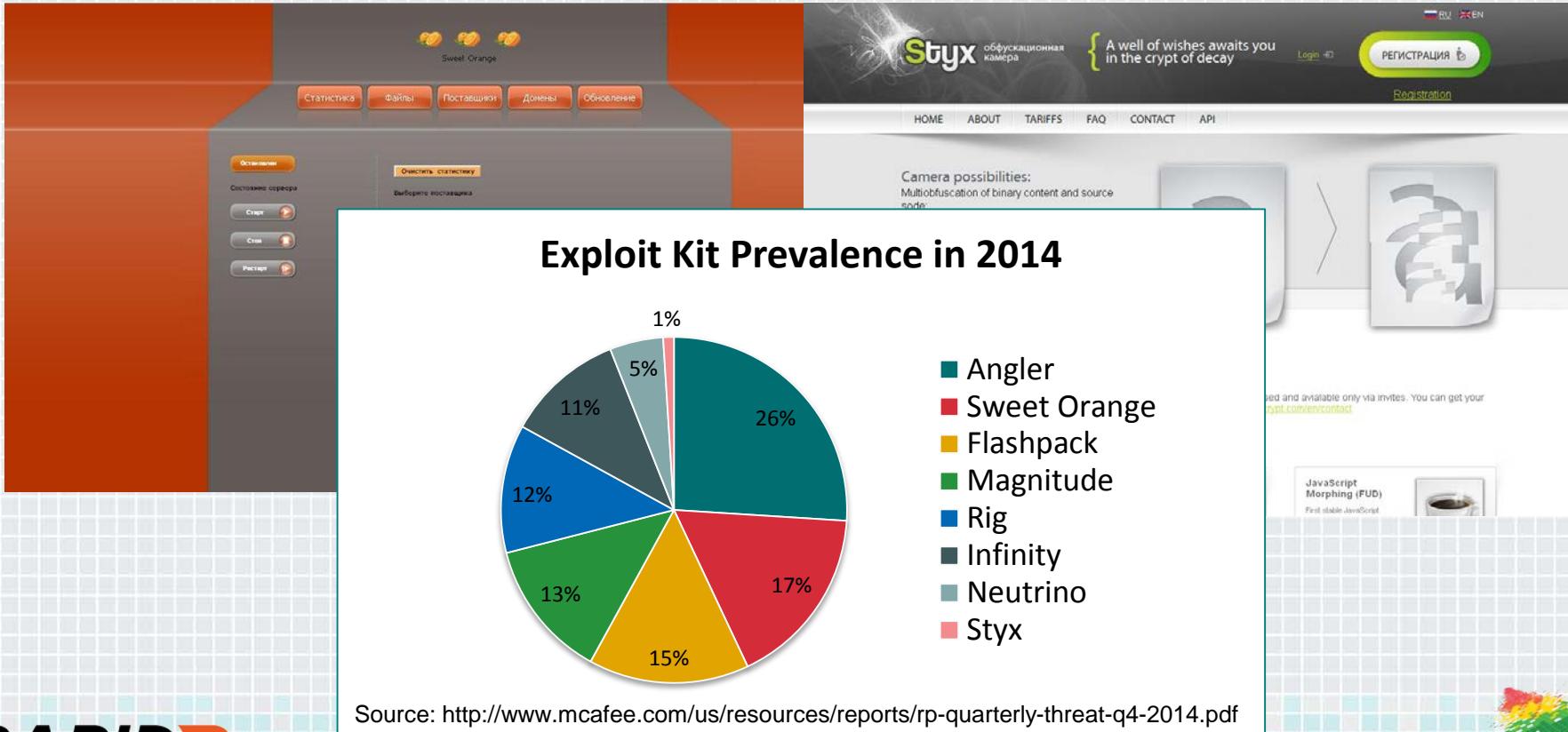


Source: Verizon 2015 Data Breach Investigations Report

# Professions in Cyber Crime

- ◆ Intruders
- ◆ Malware Developers
- ◆ Exploit Kits Developers
- ◆ Bulletproof Hosting
- ◆ Money Laundering Providers
- ◆ Traffic Brokers
- ◆ ...

# Malware: There's an App For That



# Goal: Making Money

## Profits remain high

- ◆ Credit card numbers & CVV – US\$0.50 to \$20
- ◆ Fullz (identity and financial info) – US\$30 to \$45
- ◆ Cloud Accounts – US\$7 to \$8
- ◆ Healthcare Information – US\$20

## Costs are declining

- ◆ Exploit Kits – US\$100 to US\$700/week
- ◆ DDoS Attacks – US\$10 to \$1000/day
- ◆ Infected Computers – US\$140 to \$190/1,000

Dec 2014 - Source: <http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>  
Dec 2014 - Source: [http://www.secureworks.com/resources/articles/featured\\_articles/whitepaper-underground-hacking-markets-report](http://www.secureworks.com/resources/articles/featured_articles/whitepaper-underground-hacking-markets-report)



# Not Just Endpoints

- ◆ Stuxnet made targeted SCADA/ICS attacks infamous



- ◆ BlackEnergy variant fueling long running ICS campaign

# Not Just Endpoints

- ◆ PCI requires encrypting card data, criminals respond with RAM-scraping malware
- ◆ 2014 continued to see Point-of-Sale malware evolving
- ◆ Default, weak and stolen credentials are a major part of Point-of-Sale breaches

# Not Just Endpoints

- ◆ ATMs are Windows machines filled with cash
- ◆ Attacks using malware on USB sticks or bootable CDs
- ◆ Estimated 75% of ATMs still run Windows XP, even after Microsoft ended support
- ◆ NCR launches Kalpana – Android based ATMs



# Not Just Endpoints

- ◆ Android remains the uncontested malware leader
- ◆ Malvertisements have become the primary distribution model
- ◆ But we're still waiting for the mobile malware explosion...

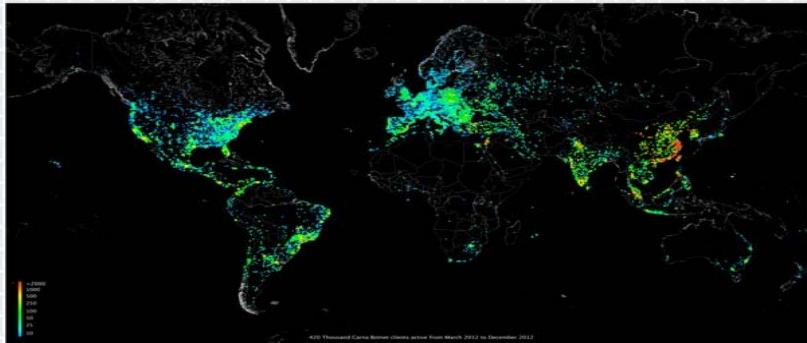


**0.03%**  
OUT OF TENS OF  
MILLIONS OF MOBILE  
DEVICES, THE  
NUMBER OF ONES  
INFECTED WITH TRULY  
MALICIOUS EXPLOITS  
WAS NEGLIGIBLE.

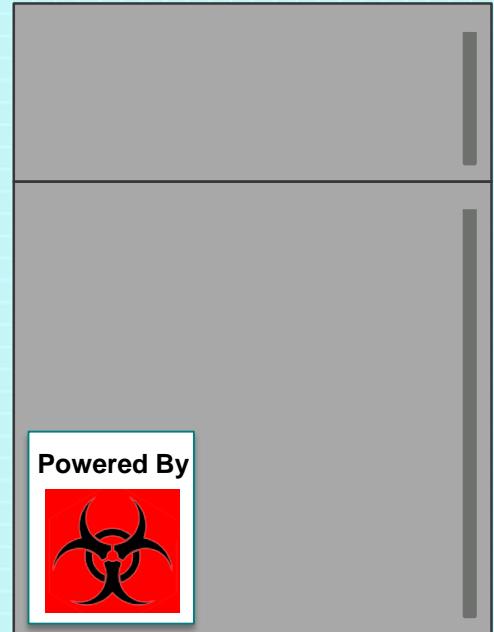
Source: Verizon 2015 Data Breach Investigation Report

# Not Just Endpoints

- ◆ Internet-of-Things botnets devolving from Internet Census to DDoS and spam
- ◆ Always on devices ripe for hijacking
- ◆ Patching is rarely a priority



<http://internetcensus2012.bitbucket.org/paper.html>



# Understanding Today's Attacks

- ◆ The economics of security favor the criminals
- ◆ Attackers increasingly rely on deception and the human element
- ◆ State-sponsored APTs are not the only targeted attacks
- ◆ Once inside, attackers become insiders
- ◆ Intrusion Kill Chains – understand attackers methodology and apply corresponding defensive measures to increase cost and complexity to the attacker

<http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

# The Intrusion Kill Chain

- ◆ Identify methods to detect, deny, disrupt, degrade, deceive, or destroy the attack within each phase

Reconnaissance

- Web Analytics, Firewall ACL

Weaponization

- NIDS, NIPS

Delivery

- Vigilant user, Proxy filter, Inline AV, Queueing

Exploitation

- HIDS, Patch, DEP

Installation

- HIDS, Sandbox/Jail, AV

Command & Control (C2)

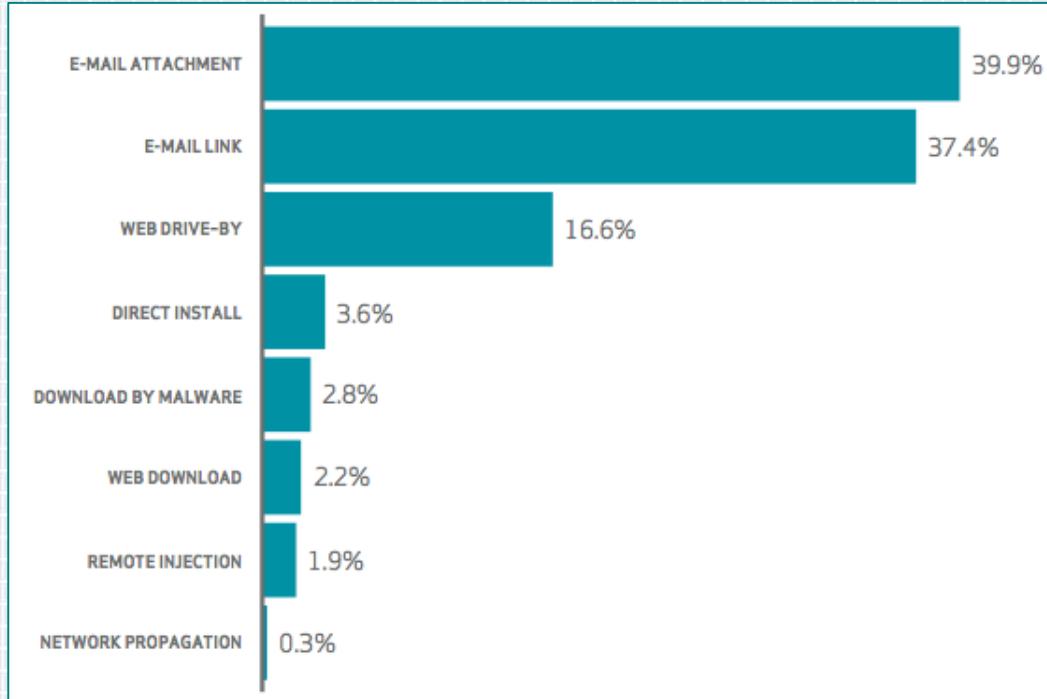
- NIDS, Firewall ACL, NIPS, Tarpit, DNS redirect

Actions on Objectives

- Audit log, QoS, Honeypot

<http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

# Malware Infection Points

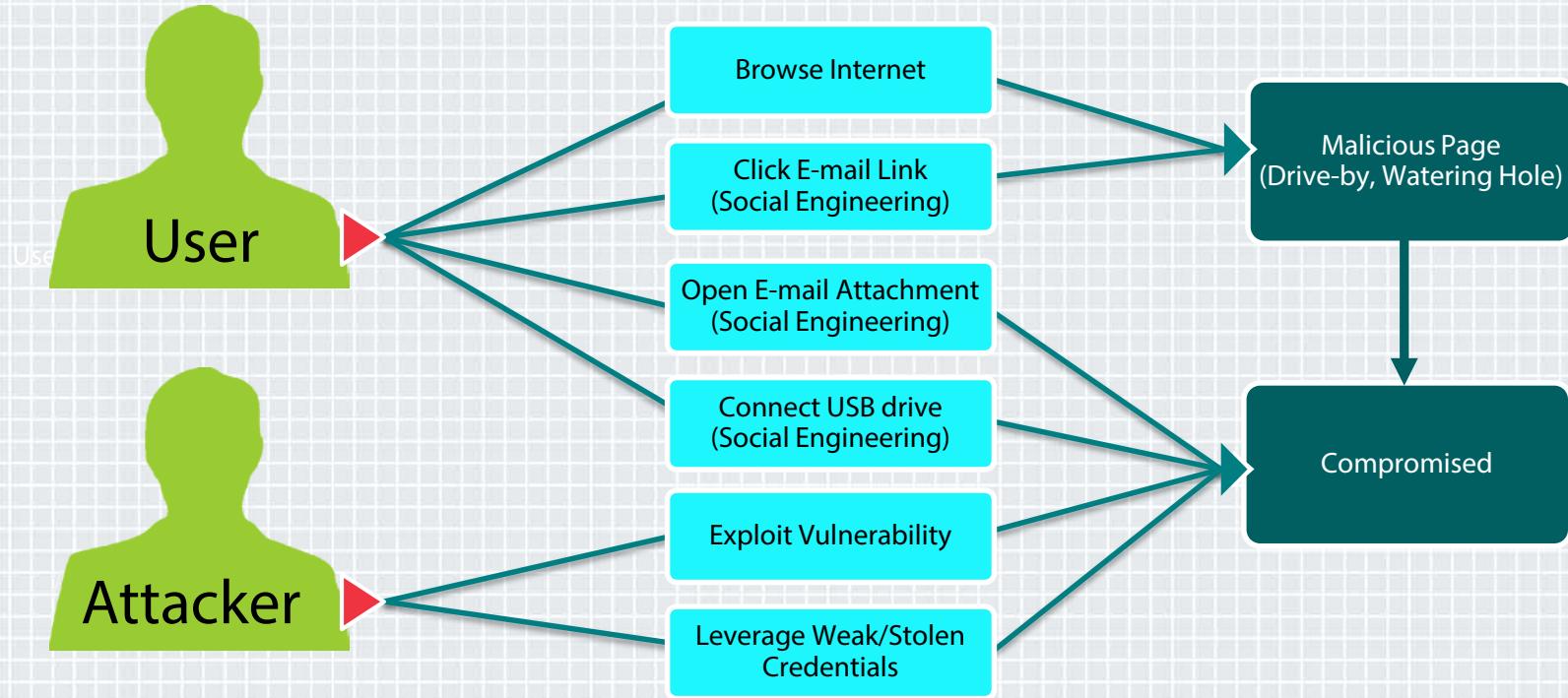


Source: Verizon 2015 Data Breach Investigations Report

**23%**  
OF RECIPIENTS NOW  
OPEN PHISHING  
MESSAGES AND  
11% CLICK ON  
ATTACHMENTS.

**50%**  
NEARLY 50% OPEN  
E-MAILS AND CLICK ON  
PHISHING LINKS WITHIN  
THE FIRST HOUR.

# Common Attack Paths



# Establish Foothold, Obtain Objective

- ◆ Communication channels for Command & Control (C2) & Data Exfiltration
  - ◆ Common protocols often used: HTTP, HTTPS, DNS, FTP
  - ◆ Encryption often simplistic (XOR, Base64, Base32, ...)
- ◆ Perform reconnaissance of internal environment
  - ◆ Identify targets and begin acquisition
- ◆ Continue lateral movement
  - ◆ Pass the hash, stolen credentials, privilege escalation

# Combating Today's Attacks

- ◆ Determined adversaries can always get in
- ◆ Philosophy shifting from prevention to detection and containment
- ◆ That said, don't forget the basics!

# Control & Monitor Traffic Flow

- ◆ Gain visibility & increase defensive/response capabilities
- ◆ Consolidate ingress & egress points – including VPN & Cloud Services
- ◆ Perimeter has expanded – apply security controls closest to resources
- ◆ Centralized & consistent logging for endpoints, services and security controls
  - ◆ Endpoints: AV/Malware Protection, FW, Authentication Logs
  - ◆ Network services: DNS, FW, VPN, Proxy, Web, Email, File, Directory, Database
  - ◆ Cloud services: Authentication & Activity Logs
  - ◆ Security controls: IDS/IPS, DLP, WAF, Malware Protection, Honeypot, Patch Management, etc.

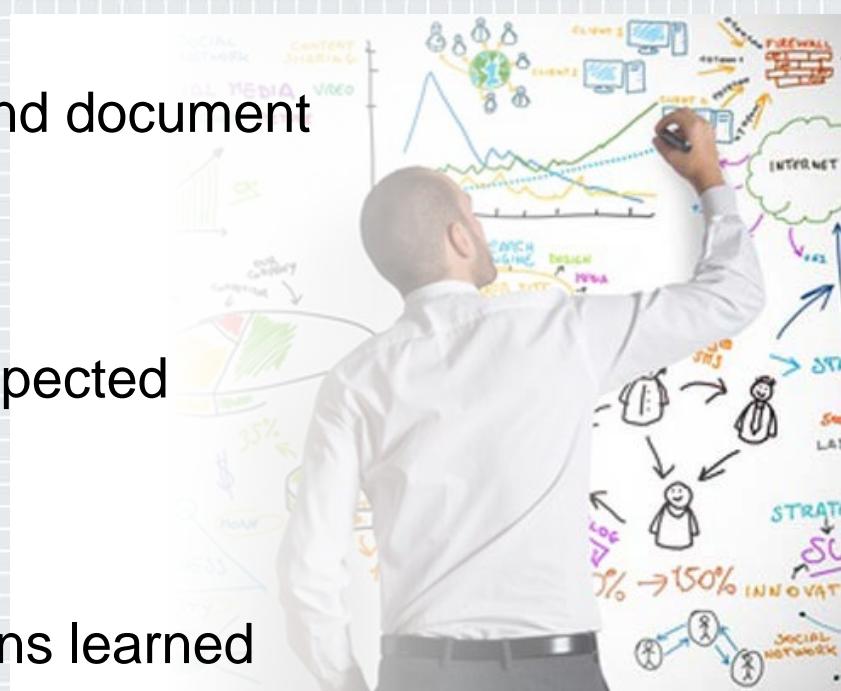


# Understand the Organization

- ◆ Correlate all activity back to users & service accounts
- ◆ Baseline the IT & user environments
  - ◆ Review inventory to identify outliers, gaps & appropriateness
- ◆ Baseline user behavior
  - ◆ Review assets users access or own for appropriateness & access patterns
- ◆ Baseline “normal” data flows
- ◆ Investigate changes, unknowns & anomalies
- ◆ Be prepared for false positives / spurious anomalies

# Preparing for Containment

- ◆ Catalog sensitive data and assets and document lockdown protocol
- ◆ Identify all points of contact
- ◆ Quarantine/monitor assets/users suspected of compromise
- ◆ Protect evidence whenever possible
- ◆ Practice & review response for lessons learned
- ◆ Refine & iterate



# The Basics: Limit User Temptation

- ◆ Rollout user awareness training, tips & advice
- ◆ Reduce spear phishing attacks – leverage Sender ID, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM)
- ◆ Deploy network-based security controls
  - ◆ Whitelist/Blacklist, Malware Protection, IDS/IPS, Proxies, Content Filtering

# The Basics: Reduce Exploit Exposure

- ◆ Automate deployment of software, patches, security controls & configurations
- ◆ Remove or patch commonly targeted applications
- ◆ Root out default/weak passwords
- ◆ Limit administrative privileges and password reuse, User Account Control (UAC)
- ◆ Enable exploit mitigations (DEP, ASLR, EMET, SEHOP)
- ◆ Deploy endpoint security controls
  - ◆ Application whitelisting, AV, FW, IPS



# Additional Reading

Lockheed Martin Corp. - Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

<http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

Contagio Malware Dump

<http://contagiodump.blogspot.com/>

Australian Signal Directorate – Strategies to Mitigate Targeted Cyber Intrusions

<http://www.asd.gov.au/infosec/top35mitigationstrategies.htm>

SANS/CSIS – Twenty Critical Security Controls for Effective Cyber Defense

<http://www.sans.org/critical-security-controls/>

# Apply

- ◆ Determined adversaries will get in – increase your focus on detection and containment, but don't forget the basics
  - ◆ Understand your business, your IT environment, your users, & the threats you face
  - ◆ Prepare your people and processes, not just technology
- ◆ Every user is part of your perimeter, treat them accordingly
- ◆ Attacks will continue to evolve – stay current and focus efforts on highest return

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

# Thank You

Tas Giakouminakis

Rapid7

Co-founder & Chief Technology Officer

[www.rapid7.com](http://www.rapid7.com)

[tas@rapid7.com](mailto:tas@rapid7.com)



# Security Basics

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	User Authentication Trends and Methods for Native Mobile Applications	Kayvan Alikhani
10:15 AM	BREAK	
10:30 AM	Mobile & IOT Security: Will Big Data Make it Better or Worse?	Hadi Nahari
11:15 AM	Viruses, Malware and Threats	Tas Giakouminakis
12:00 PM	LUNCH	
1:15 PM	Crypto 101: Encryption, Codebreaking, SSL, and Bitcoin	Benjamin Jun
2:00 PM	Security Enforcement Explained	Dana Wolf
2:45 PM	BREAK	
3:00 PM	Internet and Web Security Issues	Patrick Sullivan
3:45 PM	Network Security	Gary Sockrider

# RSA® Conference 2015

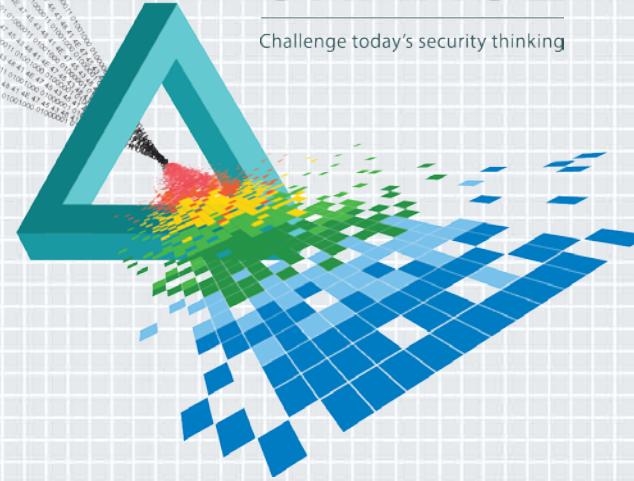
San Francisco | April 20-24 | Moscone Center

SESSION ID: SEM-M01

# Crypto 101: Encryption, Codebreaking, SSL, and Bitcoin

# CHANGE

Challenge today's security thinking



## Benjamin Jun

CTO

Chosen Plaintext Partners  
@BenjaminJun

CHOOSE  
NPLAI  
NTTEXT

#RSAC

Some material adapted from Ivan Ristic, Qualys (RSAC 2011)

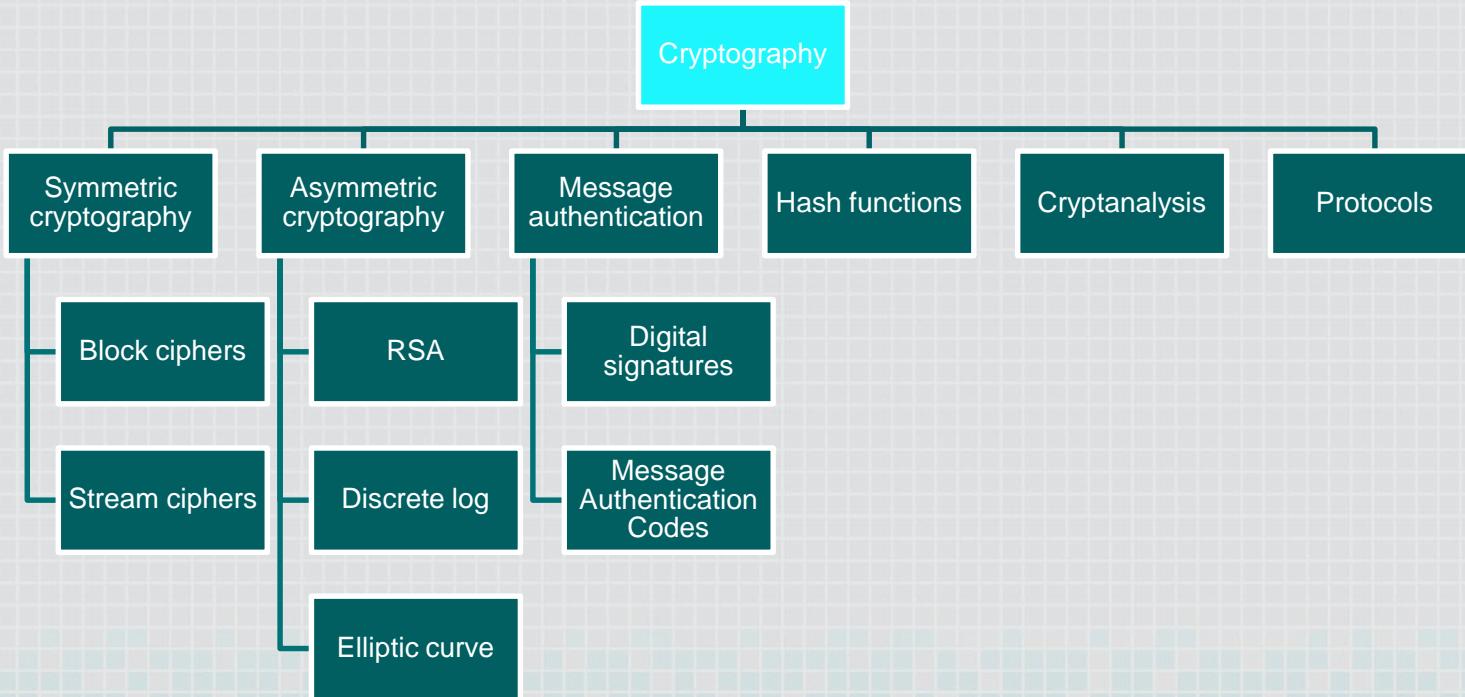
# Crypto 101

- ◆ Cryptography building blocks
- ◆ Cryptographic protocols
  - ◆ SSL / TLS
  - ◆ Bitcoin
- ◆ Attacks on cryptography



# What is Cryptography?

**Cryptography is the art and science of keeping messages secure.**



# Security \si-'kyur-ə-tē\

**the state of being free  
from danger or threat**

## Cryptography terms

- ◆ Confidentiality
- ◆ Integrity
- ◆ Authentication
- ◆ Access control
- ◆ Non-repudiation

## Other criteria

- ◆ Interoperability
- ◆ Performance
- ◆ Usability

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

# Crypto Building Blocks

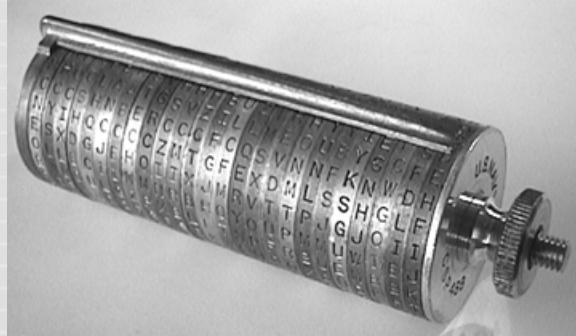


# Encryption

*Obfuscation that is fast when you know the secrets, but impossible or slow when you don't.*



Scytale  
300BC

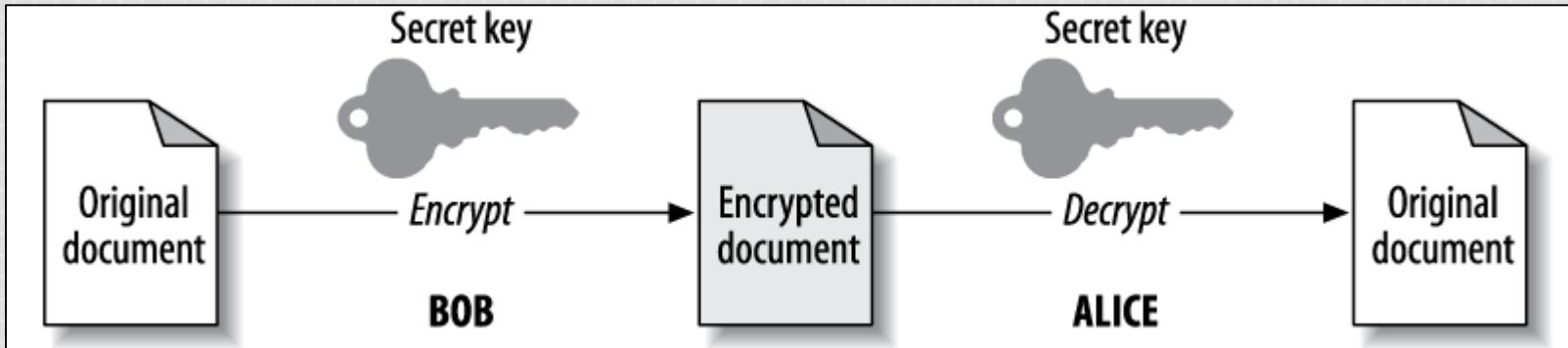


Jefferson Wheel (M94)  
1900s



Enigma Machine  
1920s

# Symmetric encryption

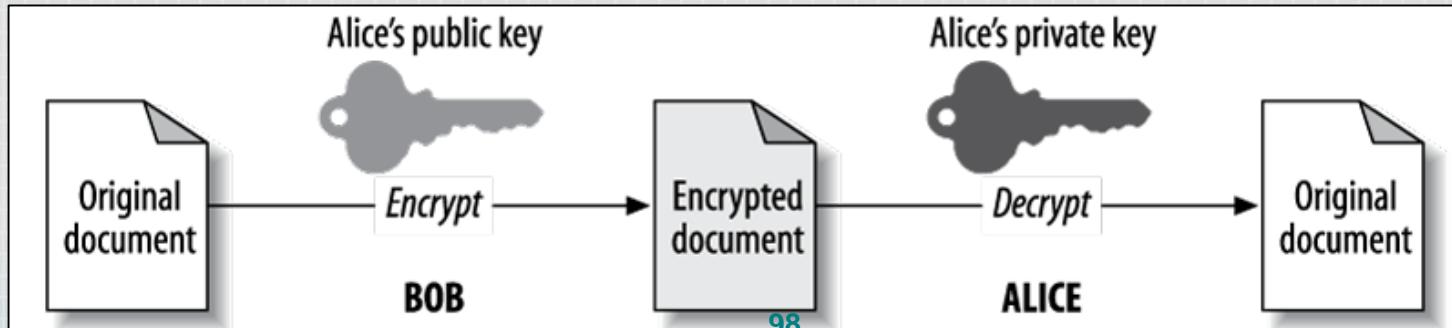


- ◆ Use shared **key** to encrypt/decrypt
  - ◆ Algorithm does not need to be secret
  - ◆ Key must be agreed and communicated in advance
- ◆ Convenient and fast
- ◆ Examples: RC4, 3DES, AES

# Asymmetric encryption

***Two related keys: one private, one public***

- ◆ Anyone with the public key can encrypt the message
- ◆ Only the private key holder can decrypt message
- ◆ Performs encryption, key exchange, and authentication
  - ◆ Examples: RSA, Diffie-Hellman, ElGamal, DSA, Elliptic curve (ECDH / ECDSA)
  - ◆ Significantly slower than symmetric encryption



# Authentication

*Confirm data integrity and message origin*



Egyptian signet ring  
(500BC)



Mark of the Fisherman  
(1200AD)

*On death, Cardinal Camerlengo to destroy*



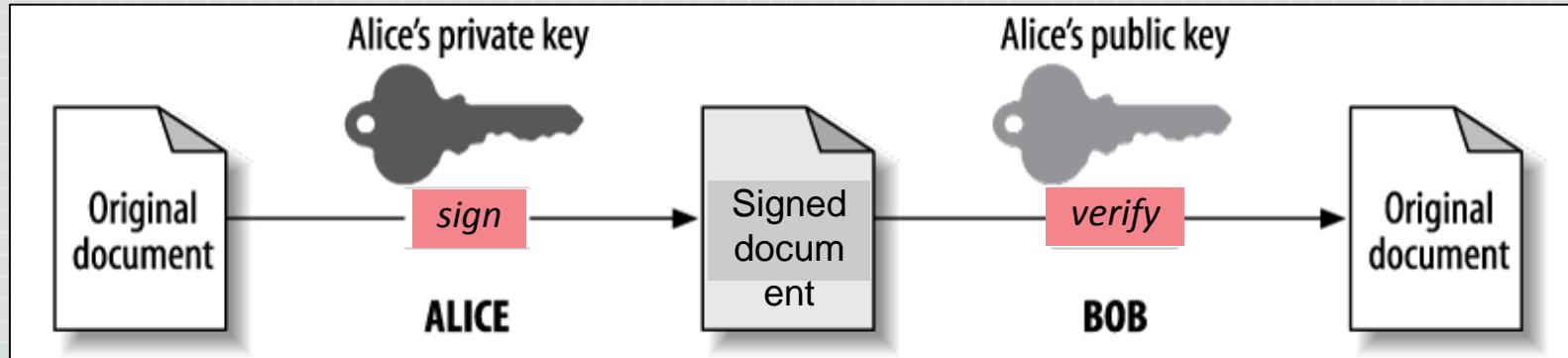
US nuclear “football”  
(present day)

*Keys roll at noon on inauguration day*

# Digital signatures

***Asymmetric cryptography can authenticate messages***

- ◆ Only the private key holder can generate a signature
- ◆ Anyone with the public key can validate the signature
- ◆ Signatures protect **digital certificates** from modification or forgery



# Digital certificates

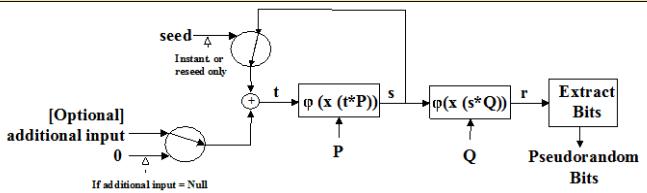
- ◆ Digital ID can include public/private keypair
- ◆ **Digital certificate** conveys identity
  - ◆ Credential holder info (name, address, etc.)
  - ◆ Identity's public key
  - ◆ Validity period
  - ◆ Digital signature of Certificate Authority (CA)
- ◆ Authentication has 3 steps
  - ◆ CA signature confirms data is authentic, vouched for
  - ◆ Do we approve of data in the certificate?
  - ◆ Identity keypair validated to confirm ID holder has the private key



# Randomness matters

- ◆ Random numbers at the heart of crypto
  - ◆ Used for key generation
  - ◆ Weak keys = weak encryption
- ◆ Random number generators
  - ◆ True random (TRNG) – *truly random*
  - ◆ Pseudorandom (PRNG) – *look random*
    - ◆ PRNGs fine if properly seeded and properly designed

## NIST SP800-90A: Dual EC DRBG with **NIST NSA\*** constants



*(don't use these)*

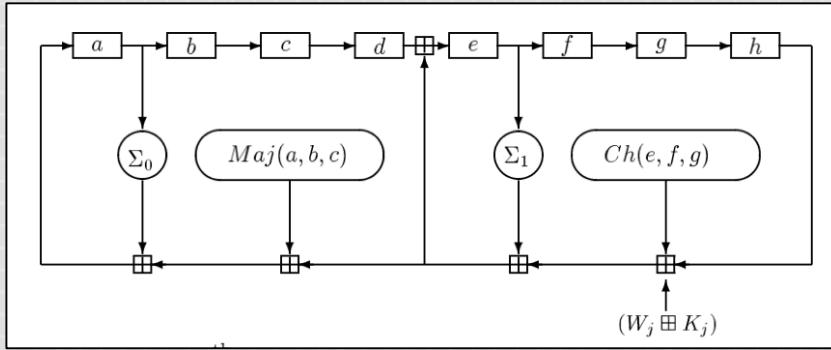
7c598 52018192

$Q_y = b28ef557\ ba31dfcb\ dd21ac46\ e2a91e3c\ 304f44cb\ 87058ada$   
 $2cb81515\ 1e610046$

\* NYT Snowden memos, September 2013

# Hash functions

- ◆ One-way transformation to generate *data fingerprints* for:
  - ◆ Digital signatures
  - ◆ Integrity validation
  - ◆ Tokenization (e.g., storing passwords)



SHA2 (SHA-256) compression function

- ◆ Examples
  - ◆ MD5 **considered broken**
  - ◆ SHA-1 (160) **some concerns**
  - ◆ SHA-2 (256) **ok**
  - ◆ Keccak and SHA-3

- ◆ Desirable qualities
  - ◆ Preimage resistance (one-wayness)
  - ◆ Collision resistance and birthday

# Stay humble

- ◆ Don't roll your own crypto
  - ◆ Failure modes subtle, catastrophic
  - ◆ Standard crypto has been strongly vetted
- ◆ Avoid unnecessary complexity
  - ◆ System only as strong as its weakest link
  - ◆ Complexity = more stuff to go wrong
- ◆ Never rely on obscurity
  - ◆ "If I can barely understand it, then it must be strong!"
  - ◆ Kerckhoffs's principle: only the key should be secure



Auguste Kerckhoffs (1835-1903)

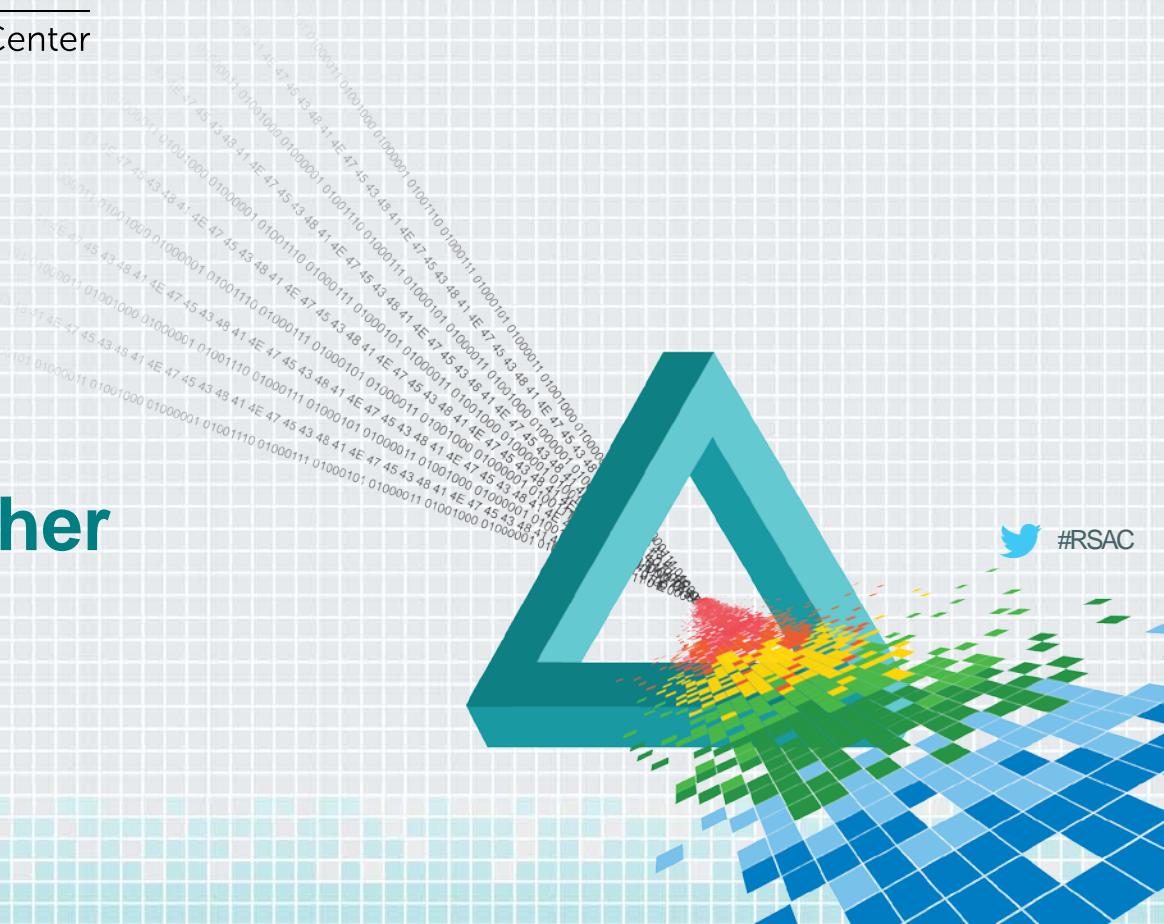


# RSA® Conference 2015

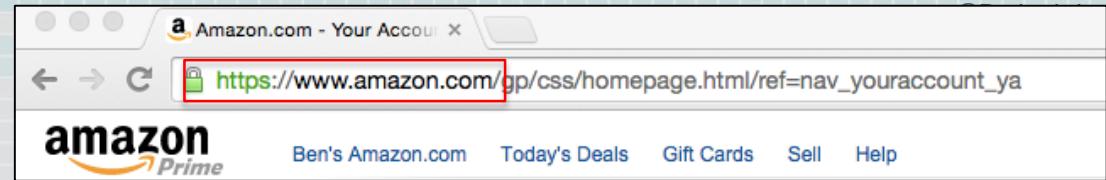
San Francisco | April 20-24 | Moscone Center

## Putting It All Together

- SSL / TLS
- Bitcoin



# TLS



- ◆ Transport Layer Security
  - ◆ World's most widely used cryptographic protocol
  - ◆ From Netscape SSL3 (Kocher, 1995)
- ◆ Security requirements
  - ◆ Securely connect with someone you have never met
  - ◆ Data privacy, data integrity, no site impersonation, no man-in-middle

# Getting to https

1. Webserver provides digital certificate to browser
  - “Amazon.com’s passport”
2. TLS layer + browser “authenticates passport”
  - Confirms data fields in cert
  - Confirms digital signature
3. TLS layer confirms that webserver holds private key
  - Sends encrypted data that can only be decrypted w/private key

https://www.amazon.com/gp/css/homepage.html/ref=nav\_youraccount\_ya

amazon

Ben's Amazon.com Today's Deals Gift Cards Sell Help

Organization Amazon.com  
Common Name www.amazon

Issuer Name \_\_\_\_\_  
Country US  
Organization VeriSign, Inc.  
Organizational Unit VeriSign Trust Network  
Organizational Unit Terms of use at https://www.verisign.com/rpa (c)10  
Common Name VeriSign Class 3 Secure Server CA - G3

Serial Number 56 9D C4 F2  
Version 3

Signature Algorithm SHA-1 with RSA Encryption ( 1.2.840.113549.1.1.5 )  
Parameters none

Not Valid Before Sunday, February 1, 2015 at 4:00:00 PM Pacific Standard Time  
Not Valid After Friday, October 2, 2015 at 4:59:59 PM Pacific Daylight Time

Public Key Info  
Algorithm RSA Encryption ( 1.2.840.113549.1.1.1 )  
Parameters none  
Public Key 256 bytes : B9 33 ED 32 A7 8B 59 CD 63 72 62 34 01 C5 8C D7 AE 74 C7 E0 71 11 C2 5C 1A E8 DB CE 08 D3 E3 19 4C 91 5E A1 88 41 67 C1 E9 F8 13 85 43 80 49 C8 2

Exponent 65537  
Key Size 2048 bits  
Key Usage Verisign's digital signature

Information about Amazon

Information about Verisign

Amazon's public RSA key

Verisign's digital signature

# TLS: Connection

Certificate check passed!

TLS 1.2 protocol for secure socket & session mgmt

The screenshot shows a web browser window for Amazon.com. The address bar displays a green lock icon and the URL [https://www.amazon.com/gp/css/homepage.html/ref=nav\\_youraccount\\_ya](https://www.amazon.com/gp/css/homepage.html/ref=nav_youraccount_ya). Below the address bar, the word "amazon" is typed into the search field. The main content area has two tabs: "Permissions" and "Connection". The "Connection" tab is active, showing the following details:

- Identity verification:** The identity of the website has been verified by VeriSign Class 3 Secure Server CA - G3 but does not have public audit records. A green lock icon is shown next to this text.
- Encryption:** Your connection to www.amazon.com is encrypted with 128-bit encryption. A green lock icon is shown next to this text.
- Protocol:** The connection uses TLS 1.2.
- Key Exchange:** The connection is encrypted and authenticated using AES\_128\_GCM and uses ECDHE\_RSA as the key exchange mechanism.

Annotations from the presentation:

- A green callout points to the "Identity verification" section with the text "Certificate check passed!".
- A yellow callout points to the "Key Exchange" section with the text "TLS 1.2 protocol for secure socket & session mgmt".
- A blue callout points to the "AES\_128\_GCM for bulk data" section with the text "AES\_128\_GCM for bulk data".
- A blue callout points to the "ECDHE\_RSA for key exchange" section with the text "ECDHE\_RSA for key exchange".

**AES\_128\_GCM for bulk data**

- Symmetric crypto
- AES128 block cipher (privacy)
- Galois authentication (integrity)

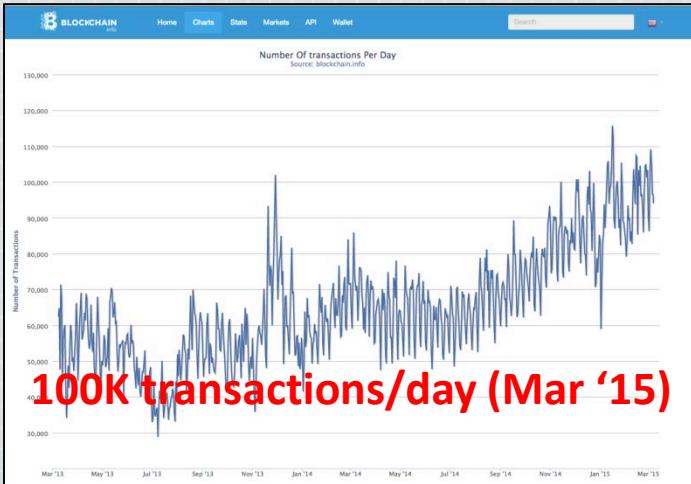
**ECDHE\_RSA for key exchange**

- Asymmetric crypto
- Confidentiality: Elliptic curve Diffie-Hellman
- Authentication: RSA2048
- “Perfect forward secrecy”

# Bitcoin (1/2)

## *A peer-to-peer, decentralized currency*

- ◆ Not underwritten by any entity
- ◆ “Satoshi Nakamoto” paper (2008)



# Bitcoin (2/2)

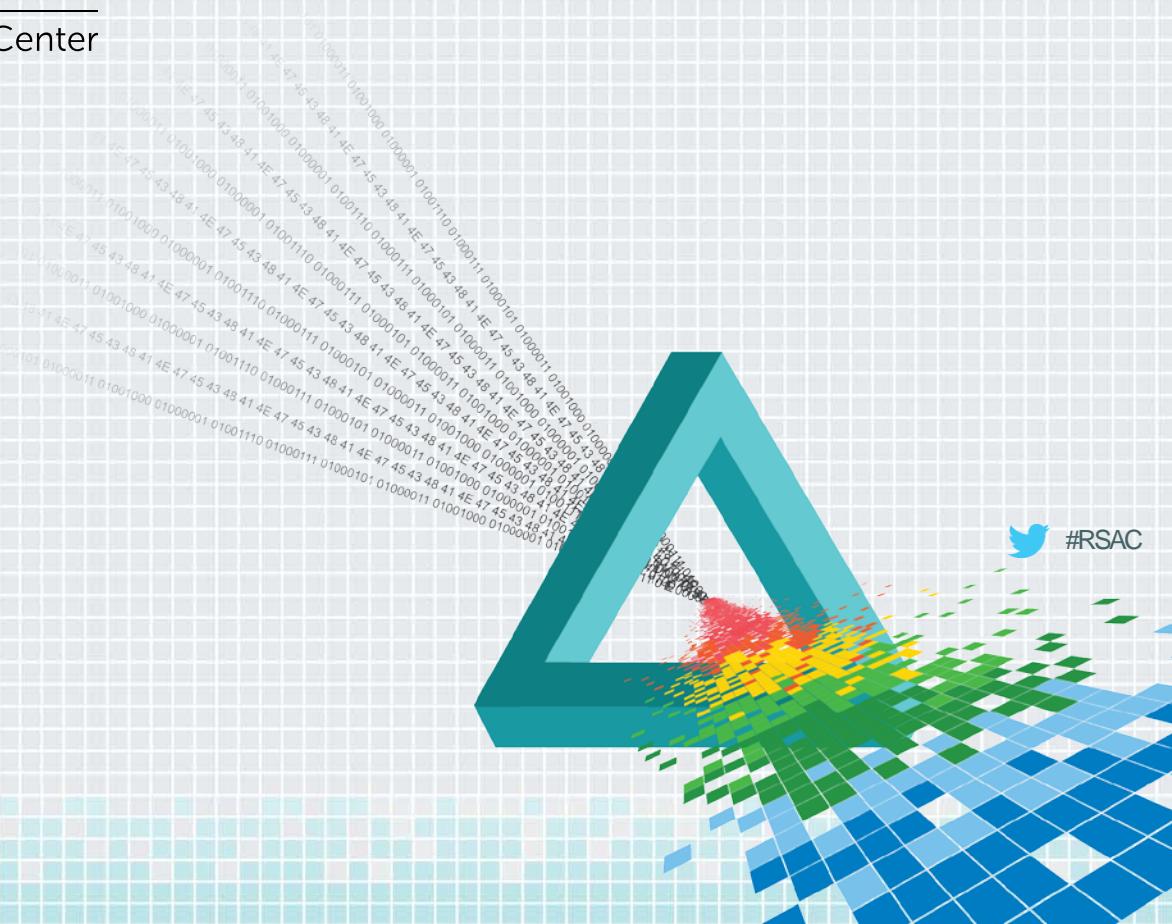
Characteristic	What happens	Cryptography
<b>Value creation</b>	Mined by searching for magic values $KWh \rightarrow BTC !$	<b>Proof-of-work</b> method uses <b>SHA-256 hash function</b>
<b>Coin transfers</b>	Digital signatures	<b>ECDSA digital signature</b>
<b>Recordkeeping (no double-spending)</b>	Distributed ledger with financial incentive for a “single view”	<b>Block chain</b> uses <b>SHA-256 hash function</b>
<b>Backing entity</b>	NONE!	<i>Everything regulated by market forces + math!</i>



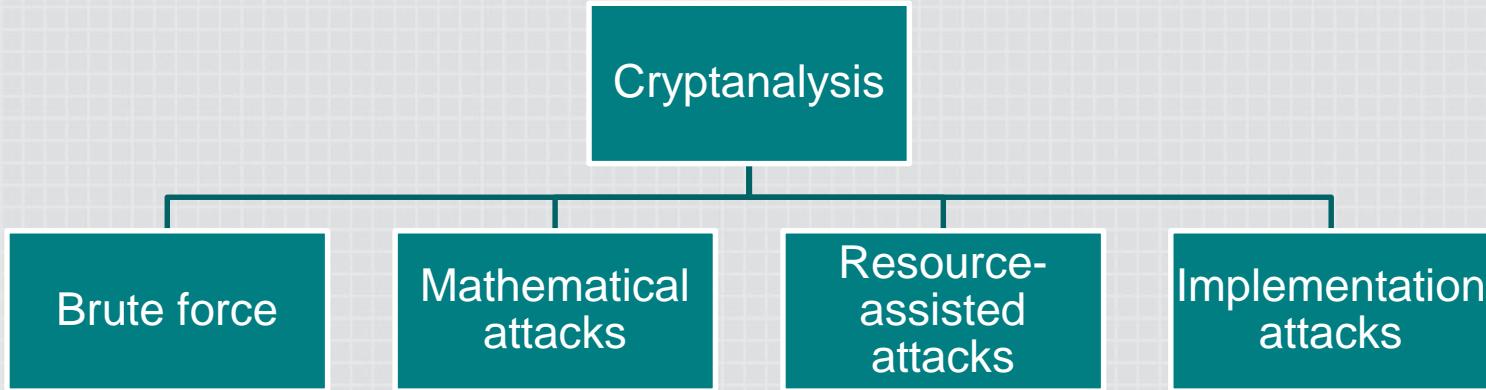
# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

## Attacks



# Attacks on cryptography



# Brute force



**US Navy Bombe, 1943**

Contains 16 four-rotor Enigma equivalents to perform exhaustive key search

CHOOSE  
NPLAI  
NTEXT



**DES Keysearch Machine, 1998**

Tests 90 billion keys/sec, average time to crack 56-bit DES: **5 days**

(Cryptography Research, AWT, EFF)

# Cryptanalysis

- ◆ HDCP = “High Bandwidth Digital Copy Protection”
- ◆ Protects digital content, interoperability
  - ◆ Fast, offline, any-to-any negotiation
  - ◆ Encryption and authentication
- ◆ “Clever” key management
  - ◆ No one device contains global secret
  - ◆ HDCP master key published (2010)
  - ◆ **Unlicensed implementations cannot be revoked**



Number of KSVs	40	42	44	46	48	50
Prob. of Spanning $M$	.295	.773	.940	.982	.997	.999

But keys from ~40 devices can reveal the master key

A Cryptanalysis of the High-bandwidth Digital Content Protection System (Crosby, Goldberg, Johnson, Song, Wagner)

# Implementation: Side Channel (1/2)

*Simple EM attack with radio at distance of 10 feet*

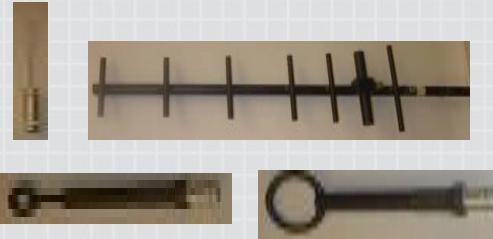
Devices



Signal Processing  
(demodulation, filtering)



Antennas



Digitizer,  
GNU Radio peripheral  
(\$1000)



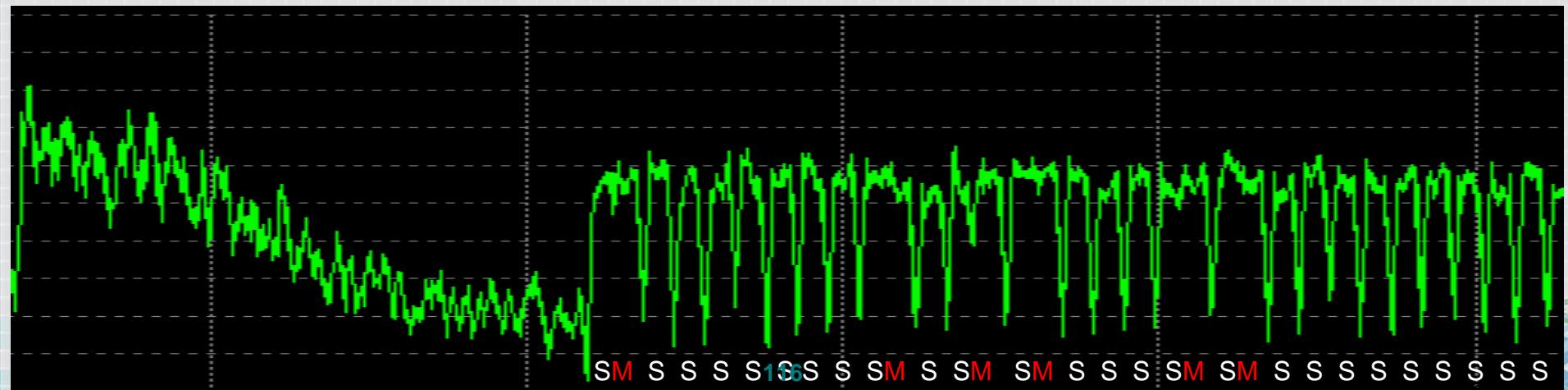
Receiver (\$350)



# Implementation: Side Channel (2/2)

- ◆ Focus on  $Mp^{dp} \bmod p$  calculation ( $Mq^{dq} \bmod q$  similar)

```
For each bit i of secret dp
    perform “Square”
    if (bit i == 1)
        perform “Multiply”
    endif
endfor
```

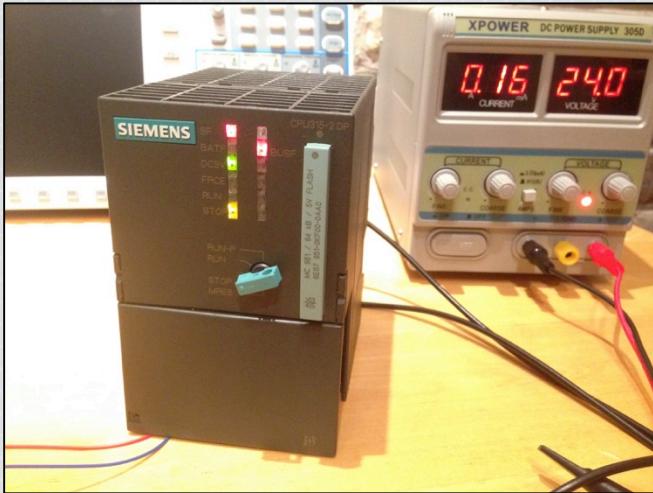


# Crypto necessary, but not sufficient



**Game King poker (2014)**

Bug allows user to adjust bet  
after hand played



**Siemens Simatic S7-315**

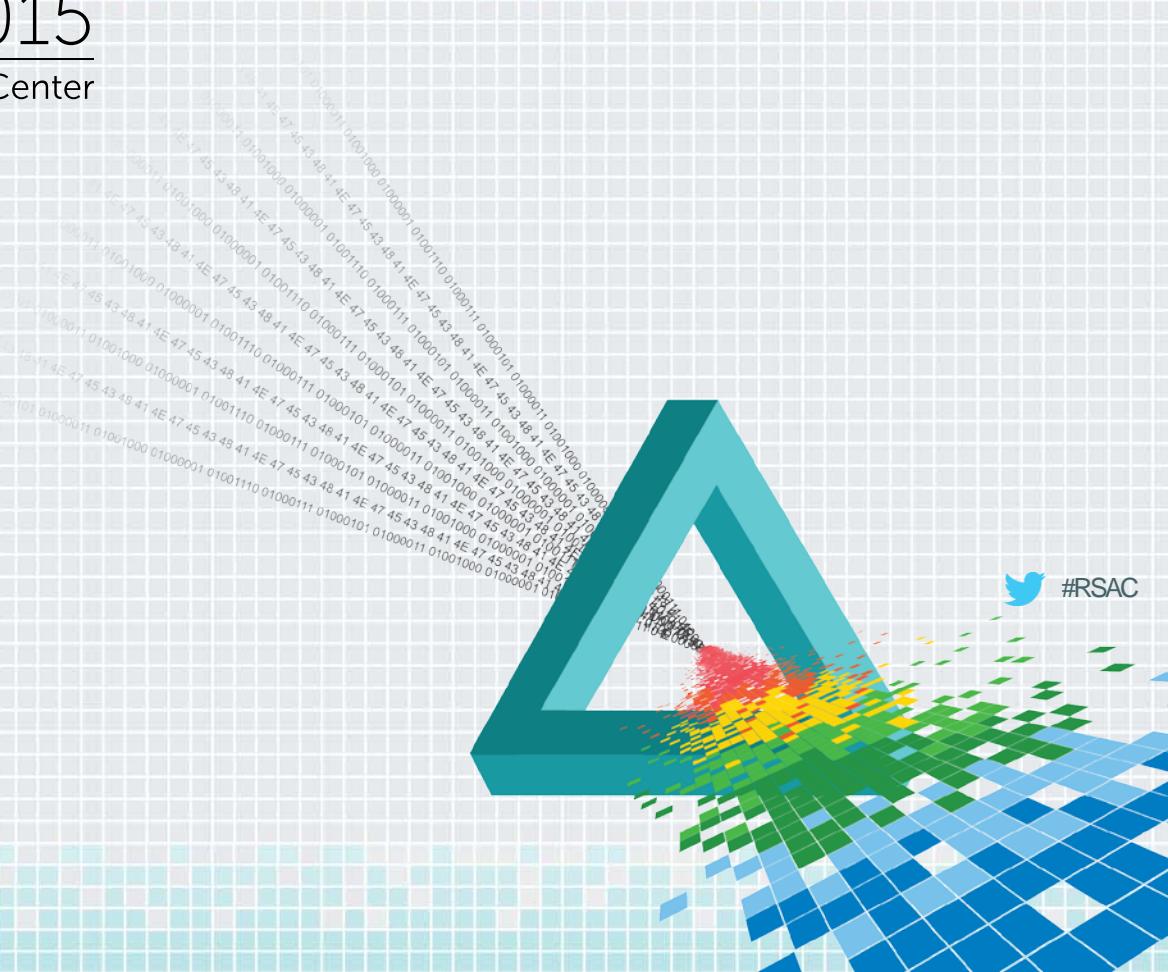
Target of Stuxnet  
Operation Olympic Games



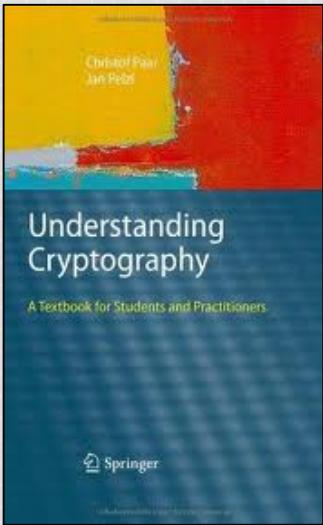
# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

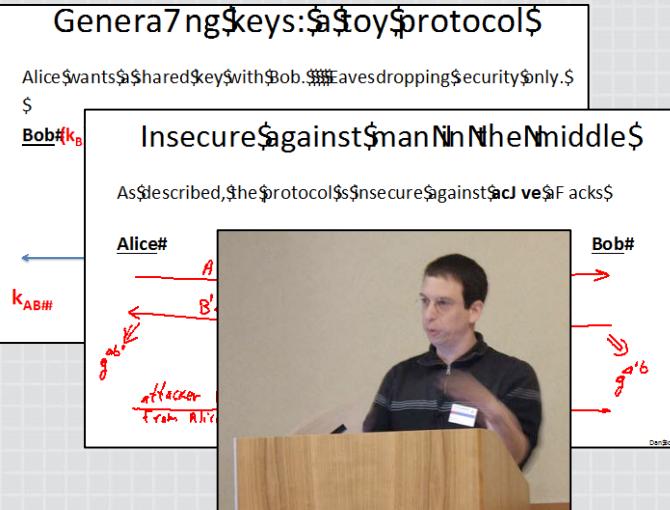
## Learn More!



# Resources



**Understanding Cryptography**  
Christof Paar and Jan Pelzl  
(Springer, 2009)



**Cryptography online course**  
Dan Boneh, Stanford University

# How to apply what you have learned

- ◆ In the first three months:
  - ◆ Identify where cryptography is used in your organization
  - ◆ Identify infrastructure required (key management, certificates)
- ◆ Within six months:
  - ◆ Know what crypto can do. Explain the different security properties.
  - ◆ Know what crypto can't do. Understand basic implementation security issues.



**CHOOSE  
NPLAI  
NTEXT**

Benjamin Jun

@BenjaminJun / ben@ChosenPlaintext.com

Chosen Plaintext Partners

**Questions?**

My talks this week:

## **Endpoints in the New Age: Apps, Mobility, and the Internet of Things**

*Securing the Ecosystem ECO-T07R*

*Tuesday 1:10pm, Thursday 10:20am*

## **Supply Chain as an Attack Chain: Key Lessons to Secure Your Business**

*Security Strategy STR-F03*

*Friday 11:20am*

# Security Basics

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	User Authentication Trends and Methods for Native Mobile Applications	Kayvan Alikhani
10:15 AM	BREAK	
10:30 AM	Mobile & IOT Security: Will Big Data Make it Better or Worse?	Hadi Nahari
11:15 AM	Viruses, Malware and Threats	Tas Giakouminakis
12:00 PM	LUNCH	
1:15 PM	Crypto 101: Encryption, Codebreaking, SSL, and Bitcoin	Benjamin Jun
2:00 PM	Security Enforcement Explained	Dana Wolf
2:45 PM	BREAK	
3:00 PM	Internet and Web Security Issues	Patrick Sullivan
3:45 PM	Network Security	Gary Sockrider

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SEM-M01

## Security Enforcement Explained

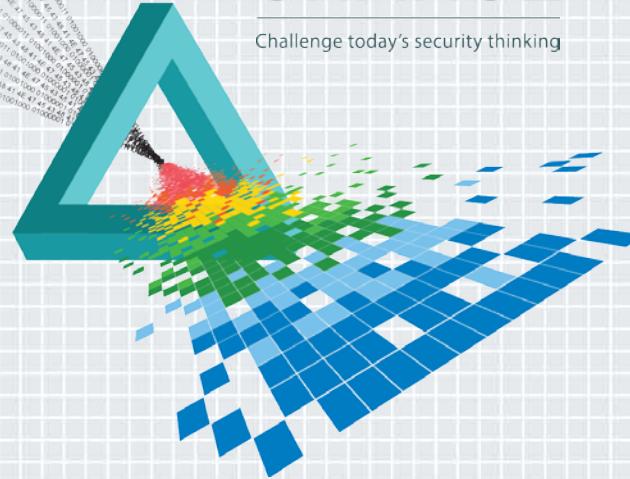
Dana Elizabeth Wolf

---

Sr. Director of Products  
OpenDNS  
@dayowolf

# CHANGE

Challenge today's security thinking



# What do we need to run a successful security program?



FIREWALL (NETWORK)



ANTI-VIRUS (ENDPOINT)

# Done. Right?



# IT Infrastructure is Changing

Elastic Process Power Due to Cloud & Virtualization



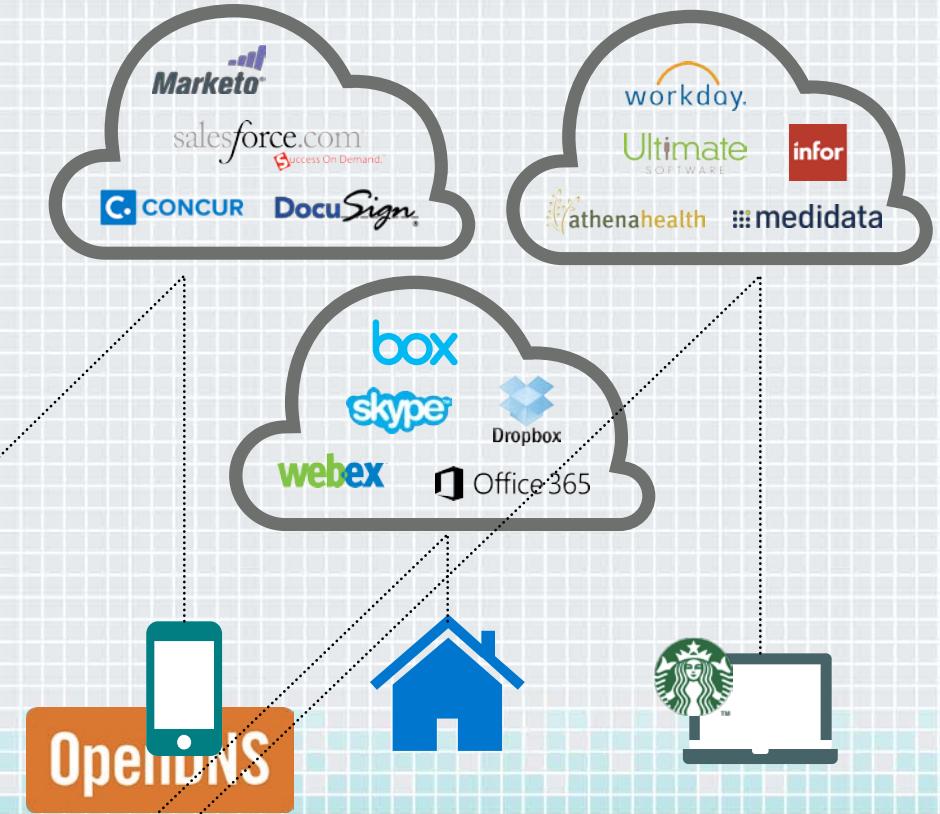
# Information Access is Changing

BYOD, Mobile, Work@Home



# Time to upgrade your thinking

...and security approach.



# Security is Changing and how we enforce policies

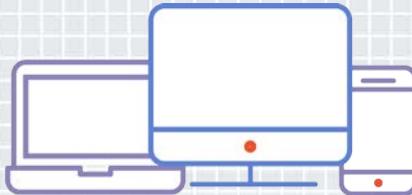


# What are we talking about?

- Key tenants of policy writing
- Policy Lifecycle or Information Security Program
- Traditional enforcement technologies
  - Endpoint
  - Network
- Challenges / Gaps
- Cloud security enforcement: emerging options

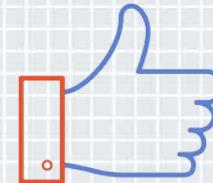
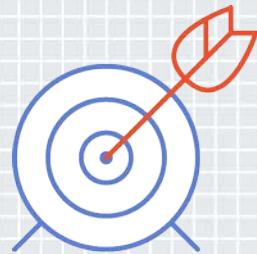
# Policy Creation

Who, What, When, Where, and Why



# Policy Creation

SMART: Specific, Measurable, Agreeable, Realistic, Time-Bound



# Security Policy Standards

## Examples

- **ISO 27001:** information security management system standard
- **Standard of Good Practice (SoGP):** business-focused, practical and comprehensive guide to identifying and managing information security risks in organizations and their supply chains
- **NIST 800-12:** helps readers understand security needs and develop sound selection of security controls

# Policy Creation & Enforcement Rules

## Positive

Whitelist



- Default: do not allow anything to pass
- Rules: what you want to permit to pass
- Typically used by: Firewalls
- Pros: More secure; can stop newer/advanced attacks
- Cons: More work to manage
- Example: Application on iPhone

# Policy Creation & Enforcement Rules

## Negative

Blacklist



- Default: allow everything to pass
- Rules: what you want to block
- Typically used by: Anti-Virus; Web Proxies
- Pros: Less work from management POV
- Cons: Less secure
- Example: No fly-list

# Policy Life Cycle

- Review logs, metrics, audits, SLAs
- Assess goal accomplishments
- Develop improvement steps & Integrate



Monitor & Evaluate

## Plan & Organize



- Threat Profile
- Security & Risk Assessment
- Get Management Sign-off

- Develop & Implement Security policies
- Identify program gaps
- Implement solutions / program
- Develop Auditing & Monitoring
- Establish goals & metrics



Implementation

## Operate & Maintain



- Follow procedures
- Carry out audits
- Manage SLAs per program

# A policy, without the lifecycle



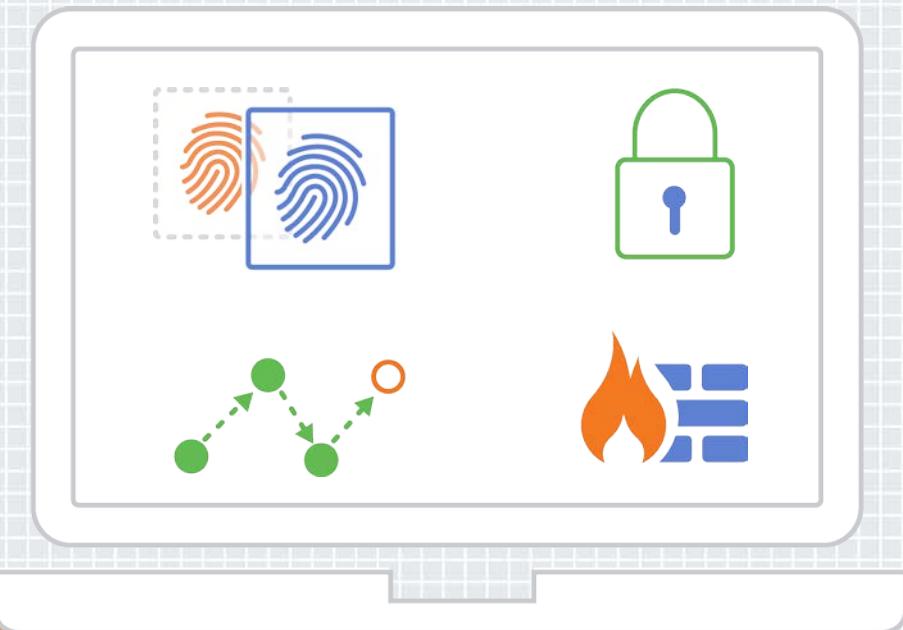
- ◆ Written and not implemented
- ◆ Disconnect & confusion around ownership
- ◆ No ROI assessment
- ◆ Missing improvement strategies
- ◆ No assurance of compliance to regulations
- ◆ Relying fully on technology as the only security solution

# Implementing Security Enforcement

- ◆ Goal
  - ◆ Consistent enforcement everywhere. No matter what!
- ◆ Challenges
  - ◆ Attackers look for (and expect) gaps in policy management & enforcement
  - ◆ Threat analysis needing more processing power

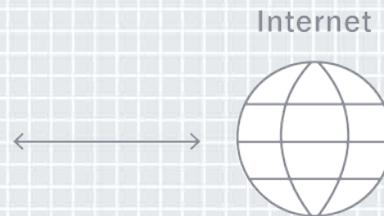
# Endpoint Security

## How Agents Work



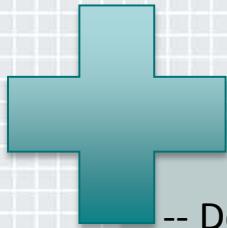
### How it works

- Two Modes
  - Interactive
  - Scan
- Signature/Rules reside on endpoint
- Stops file from doing something “bad”



# Endpoint Security Enforcement

## Strength/Weakness



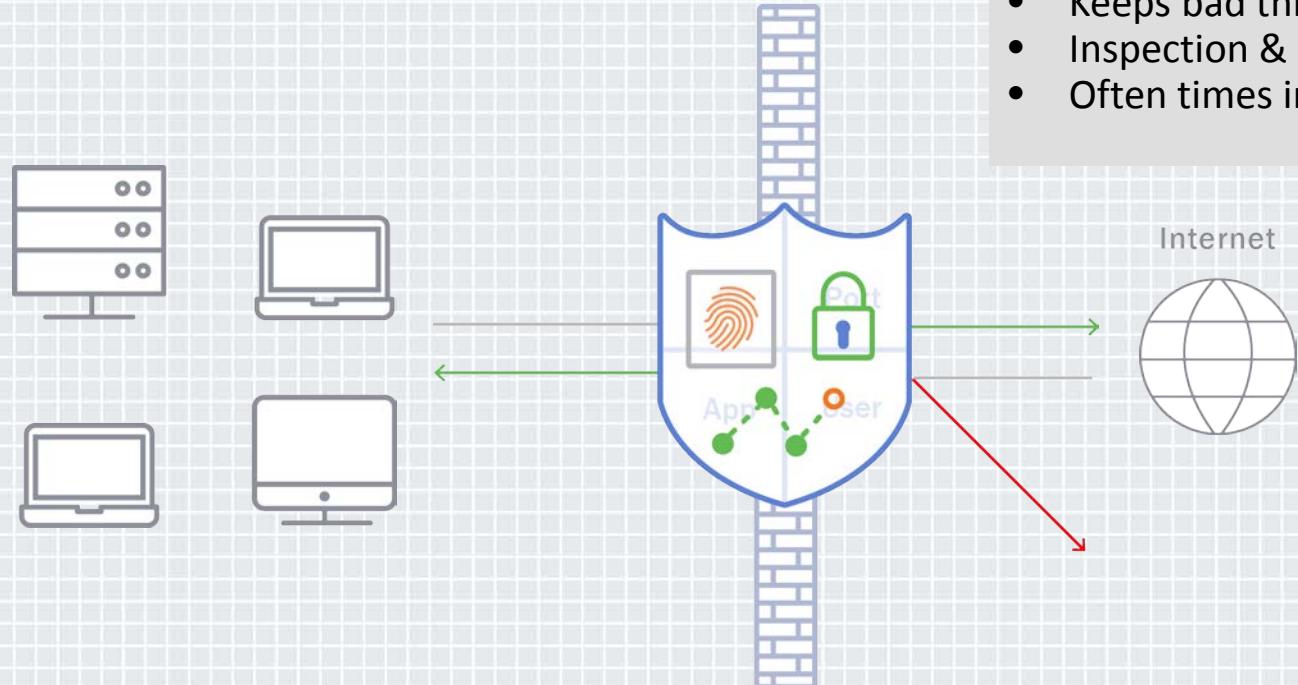
- Devices covered wherever they roam
- Visibility of inter-process communications



- Performance (policy decision & enforcement in same place)
- Deployment / Coverage
- No real-time centralized monitoring
- Manipulation by malware

# Network Security

## How Firewalls Work



### How it works

- Restricts access in/out of a system
- Keeps bad things from “spreading”
- Inspection & application based
- Often times integrating proxy

# Network Security Enforcement

## Strength/Weakness



- Hardened appliance
- Ability to segment the network into trusted zones



- Cannot protect what it cannot see
- Performance with backhauling
- Availability issues are the customer's responsibility

# In Summary

- ◆ Endpoint enforcement has limitations with management & performance
- ◆ Network enforcement has limitations with visibility & performance

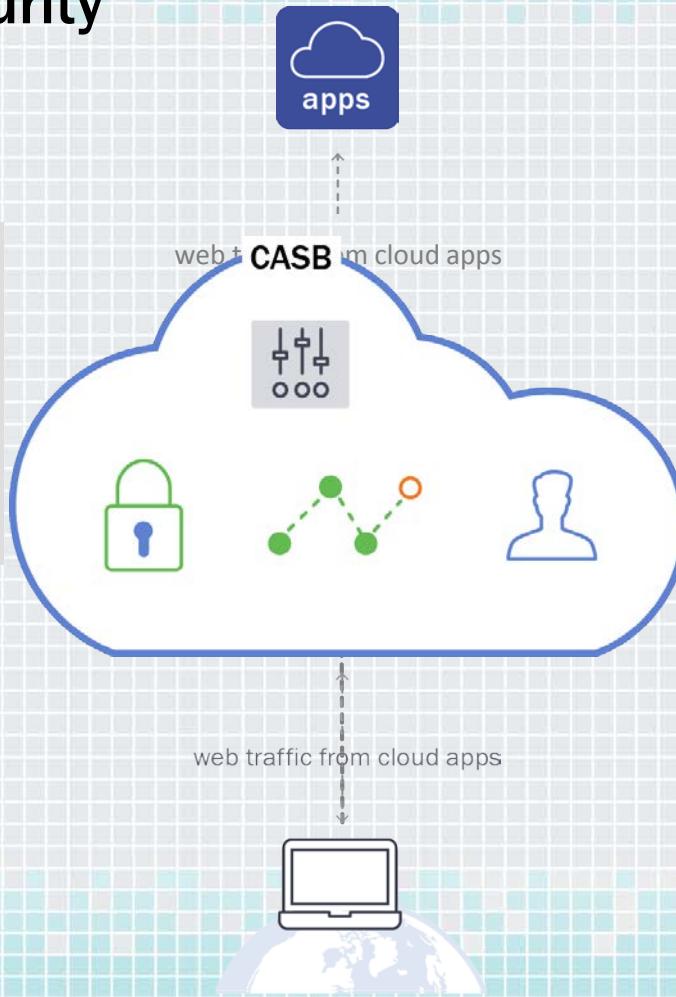
# Cloud-Delivered Security

## How CASB Works

(Cloud Access Security Broker)

### Problem It Solves

- Visibility as workloads move to cloud
- Protect application/data that is in the cloud
- Performance & processing



### How It Works

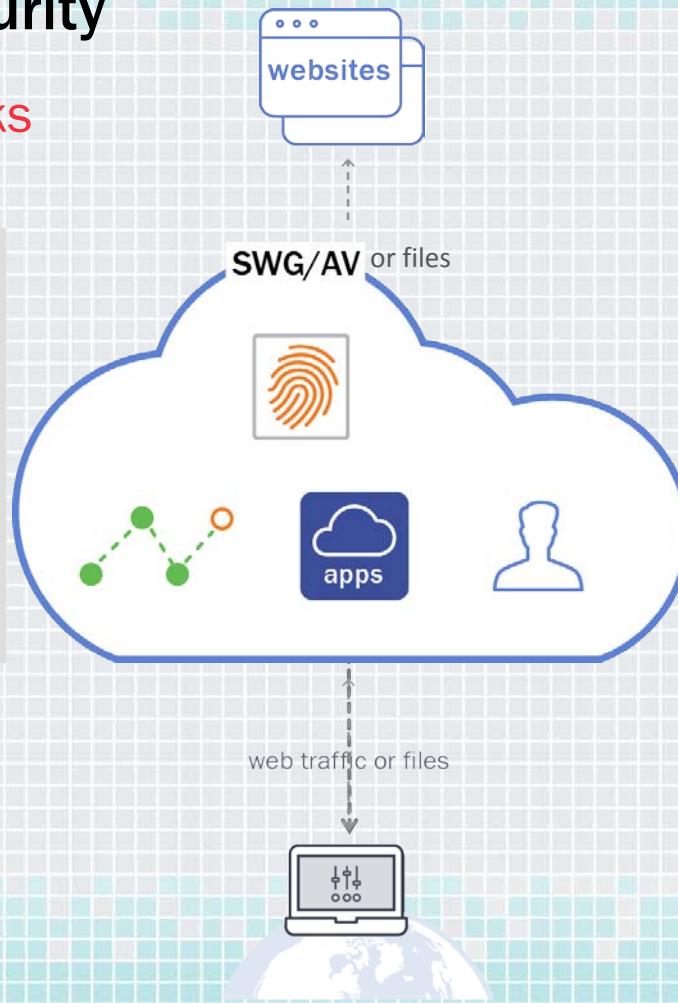
- SAML integration or reverse proxy directs traffic to cloud servers
- Traffic is inspected and policies reviewed & enforced
- DLP, Encryption, Access Control

# Cloud-Delivered Security

## How Cloud SWG/AV Works

### Problem It Solves

- Lack of visibility when users are off-network
- Performance from advanced analytic capabilities
- Performance issues from backhauling
- Manageability of intelligence updates



### How It Works

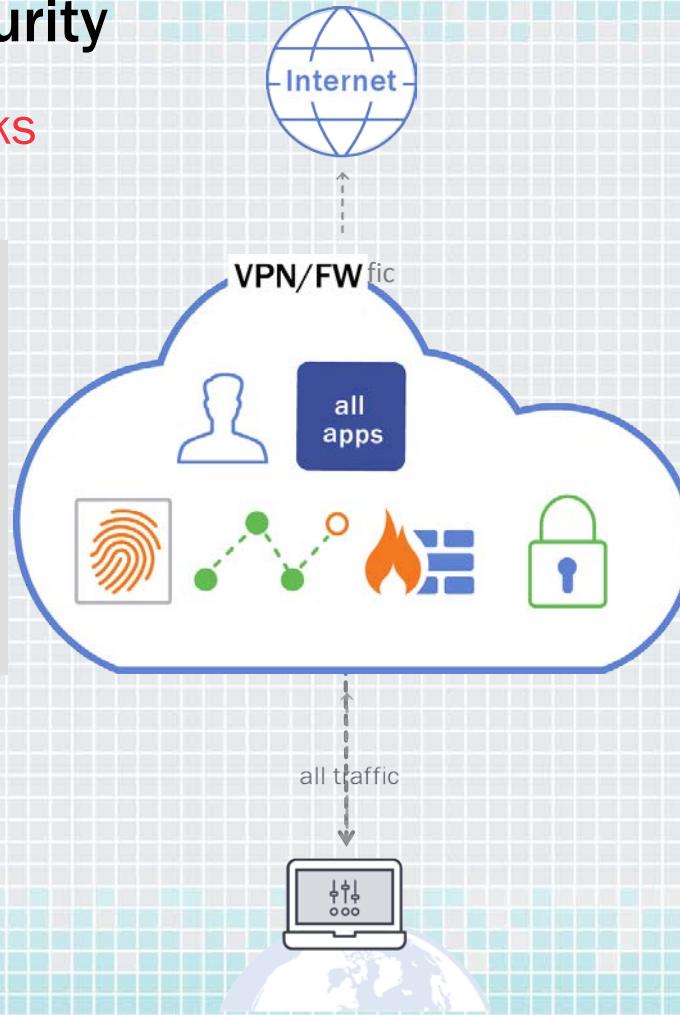
- PAC file or small agent deployed on endpoint
- Selective information or traffic sent to cloud
- All processing, policy application in the cloud
- Centralized management & reporting in the cloud
- Global network: cloud is closer to customer

# Cloud-Delivered Security

## How Cloud VPN/FW Works

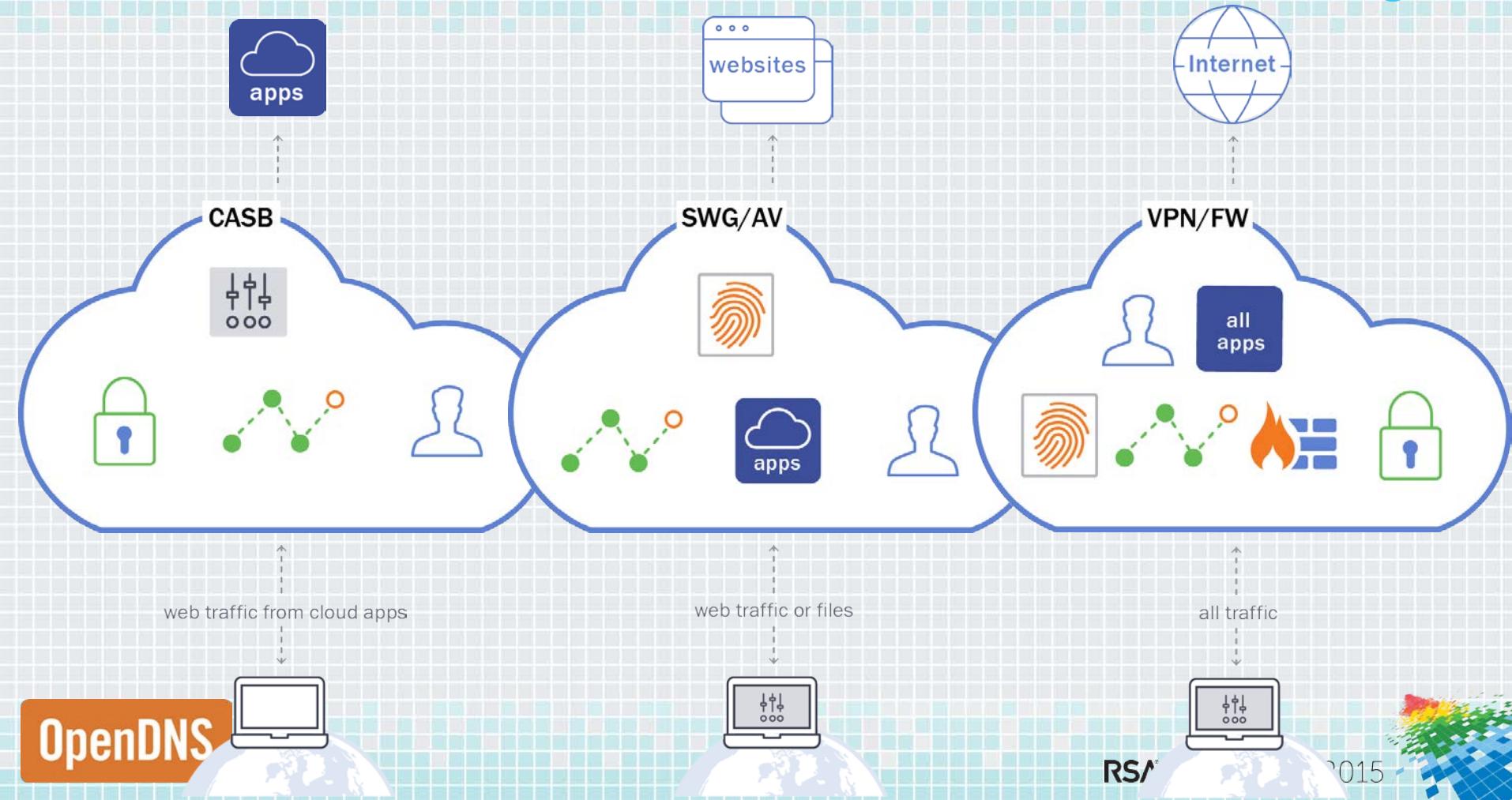
### Problem It Solves

- Visibility on & off-network and all packets
- Encryption of all traffic
- Performance from advanced analytic capabilities
- Performance issues from backhauling
- Manageability of intelligence updates



### How It Works

- Small Cloud VPN on endpoint or router
- Intelligently routes traffic
- Encrypts traffic as necessary
- All processing, policy application in the cloud
- Centralized management & reporting in the cloud
- Move all network security into the cloud
- Global network: cloud is closer to customer



# Challenges still exist

- ◆ Management: Endpoint deployment
- ◆ Management: BYOD device management

# Tying it together

- ◆ Implement a lightweight policy life cycle process
  - ◆ Do the security & risk assessment
  - ◆ Determine the gaps
- ◆ Work with IT and business unit managers to understand adoption of cloud and usage of roaming devices
- ◆ Assess performance of your existing security enforcement technologies
- ◆ Consider limited adoption of cloud enforcement security technologies to cover gaps

# Security Basics

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	User Authentication Trends and Methods for Native Mobile Applications	Kayvan Alikhani
10:15 AM	BREAK	
10:30 AM	Mobile & IOT Security: Will Big Data Make it Better or Worse?	Hadi Nahari
11:15 AM	Viruses, Malware and Threats	Tas Giakouminakis
12:00 PM	LUNCH	
1:15 PM	Crypto 101: Encryption, Codebreaking, SSL, and Bitcoin	Benjamin Jun
2:00 PM	Security Enforcement Explained	Dana Wolf
2:45 PM	BREAK	
3:00 PM	Internet and Web Security Issues	Patrick Sullivan
3:45 PM	Network Security	Gary Sockrider

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SEM-M01

## Internet and Web Security Issues

**Patrick Sullivan**

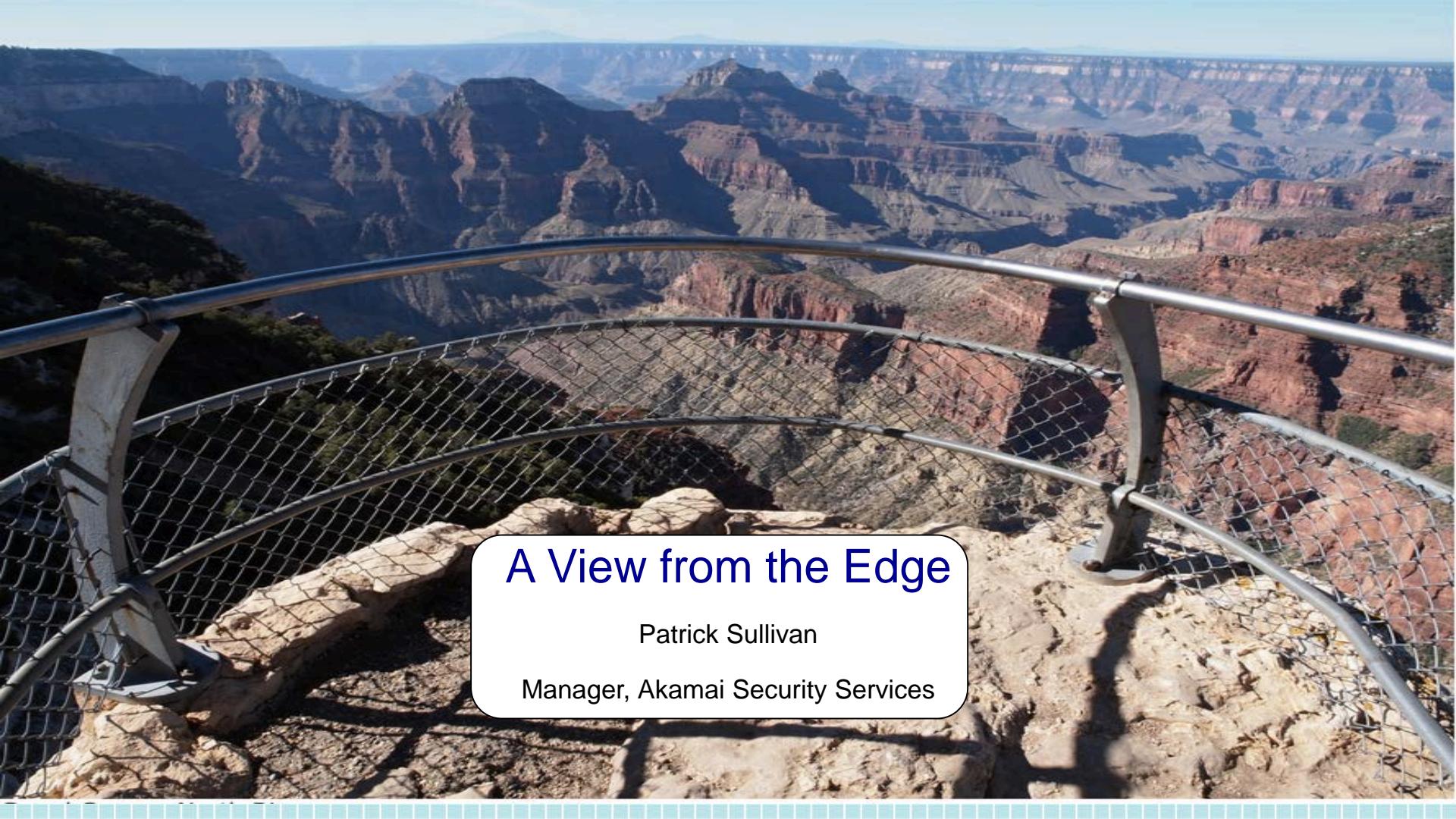
---

Manager, Akamai Security Services

# CHANGE

Challenge today's security thinking



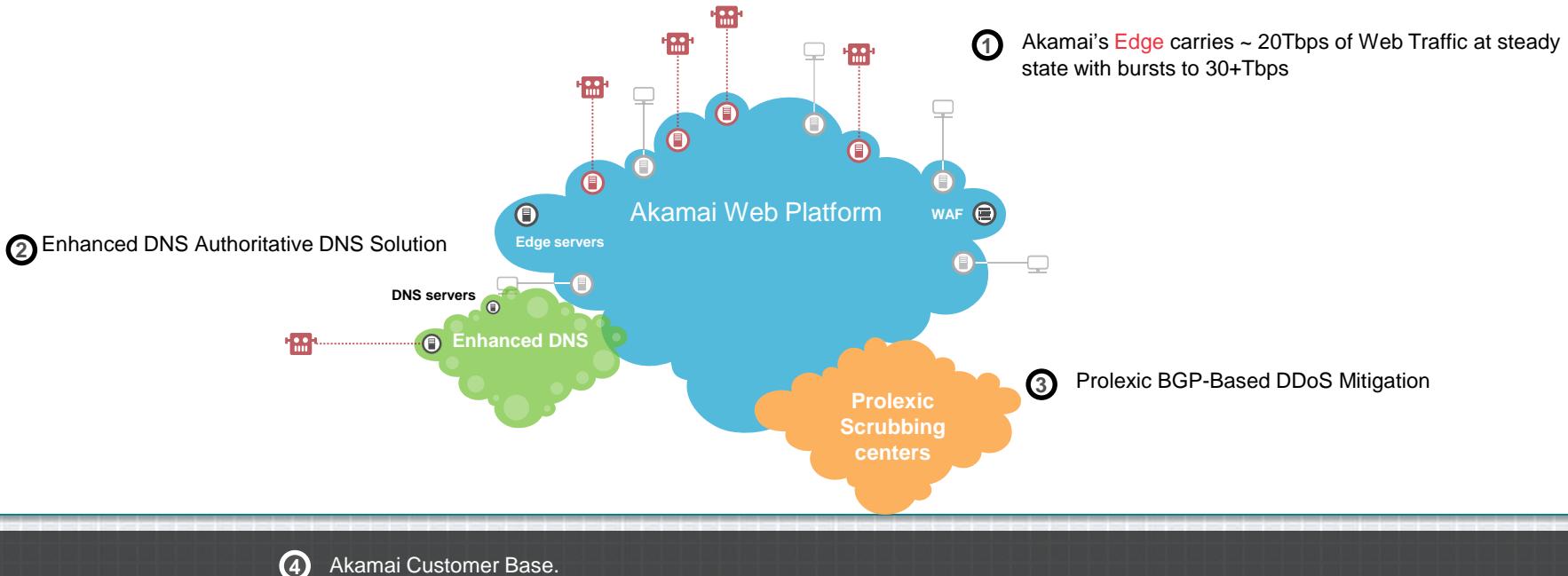


# A View from the Edge

Patrick Sullivan

Manager, Akamai Security Services

# Akamai has unique insight into Web/DDoS Traffic



- 98 of top 100 Commerce Sites
- All Branches of US Military
- All Agencies of the US Gov't
- 10 of top 10 Banks
- 30 of top 30 Media Sites
- 10 of top 10 Asset Managers
- 10 of top 10 P&C Companies
- 8 of top 10 Auto Manufacturers

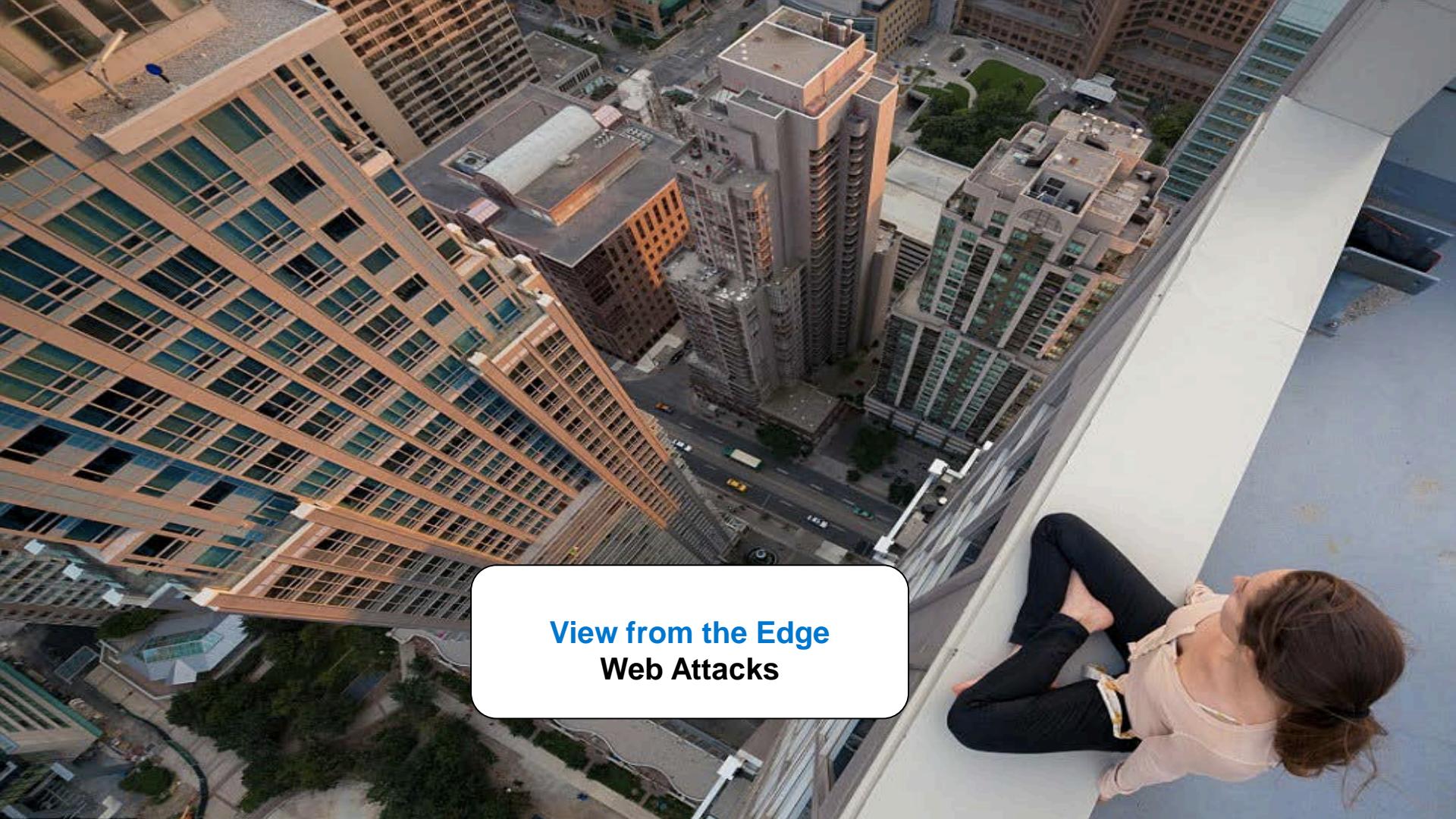
# Akamai CSI Platform Statistics

2 Petabytes of security data stored

10 Terabytes of daily attack data

# What we'll talk about today

- Web App Attacks
- DDoS Attacks
- DNS Attacks

A photograph of a woman with long brown hair, wearing a light-colored top and dark leggings, sitting on the edge of a skyscraper. She is looking down at a dense urban landscape below, which includes several modern buildings, streets with cars, and green spaces. The perspective is from high above, looking down at the city.

## **View from the Edge**

### **Web Attacks**

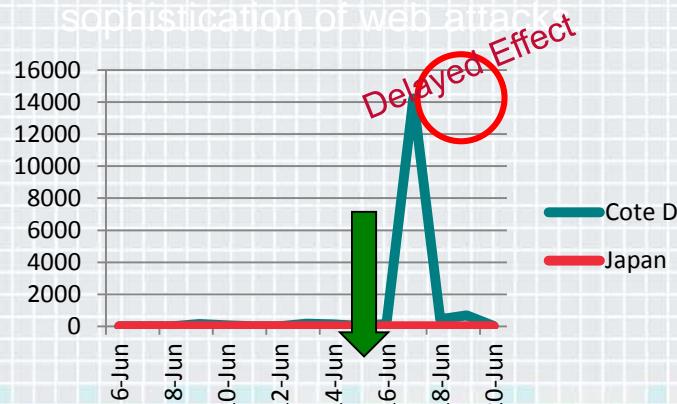
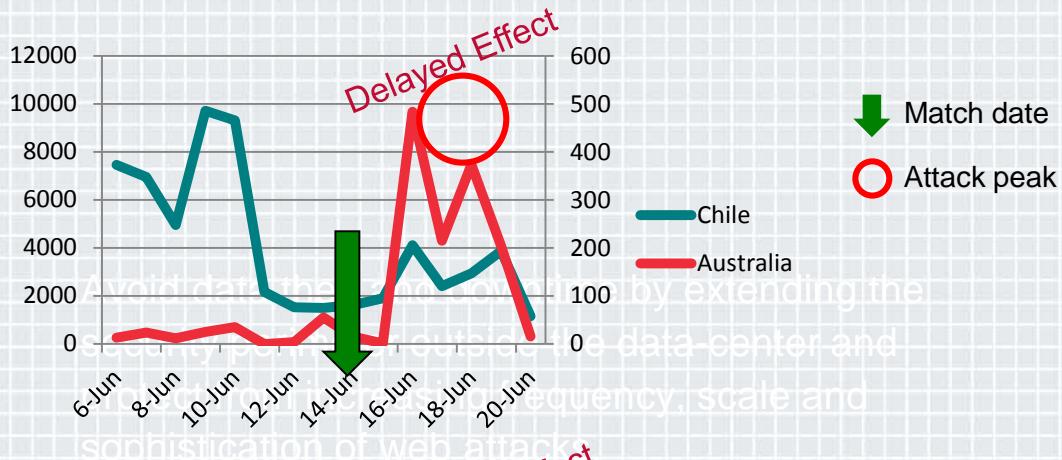
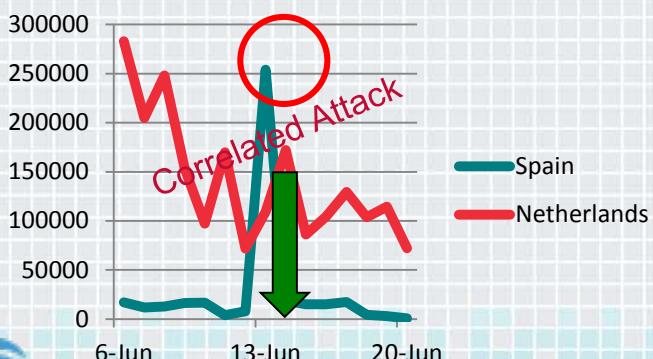
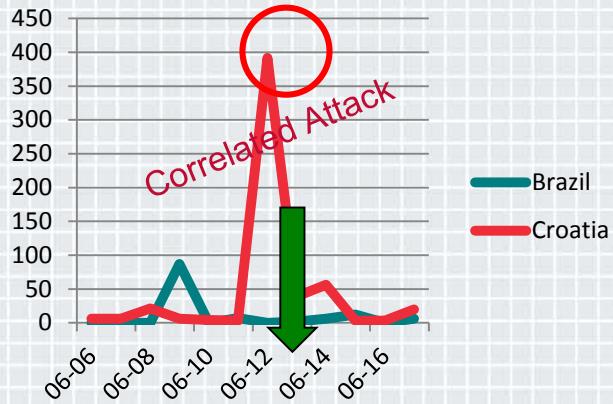
# Web Application Attacks

- Chosen Target Attacks
- Attacker picks target
  - Recon
  - Mapping
  - Discovery
  - Exploitation
  - Repeat as necessary
- Chosen Vulnerability Based Attacks
  - Attacker Picks a Vulnerability
  - Scans at massive scale
  - Beacons back when successful
  - Exploitation

# World Cup Attack Trend: Retribution Cyber Attacks



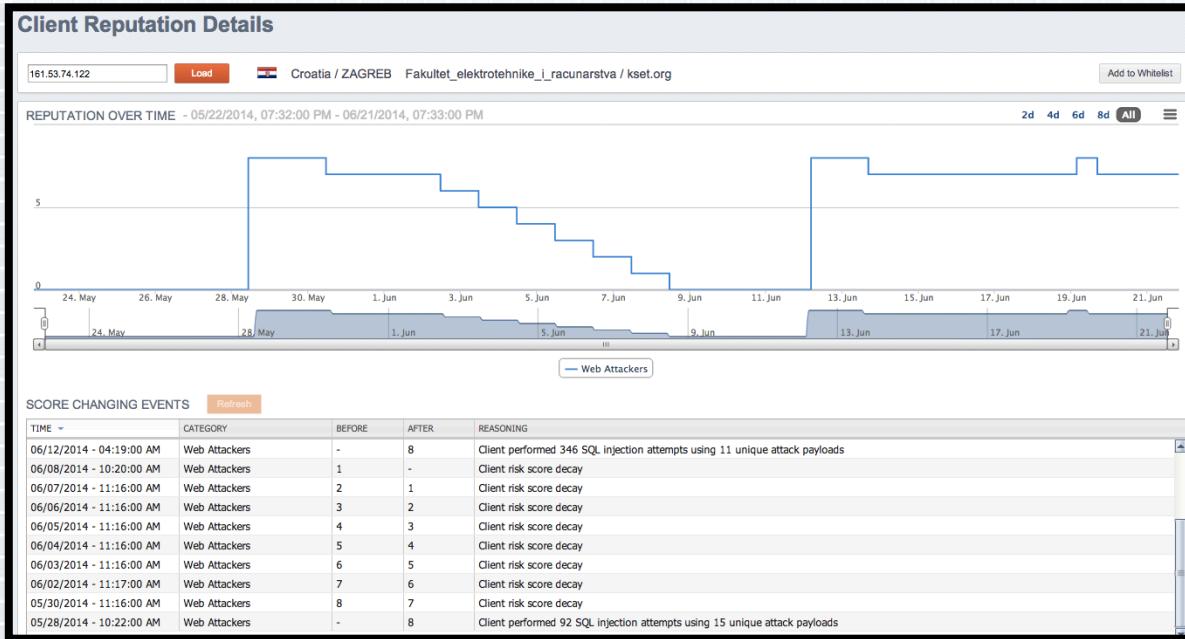
# World Cup – Correlated Events



# Croatia vs. Brazil (June 12<sup>th</sup>)



- ◆ Croatian hacker decides to retaliate – using 2 Offending IP addresses – All attacks are **real** SQL Injection attempts



EdgeScape information	
ip	217.14.208.233
country_code	HR
region_code	
county	
city	ZAGREB
zip	
timezone	GMT+1
areacode	
georegion	
network	
network_type	
company	Metronet_Telekomunikacije_d.d.
domain	vodatel.hr
fips	
lat	45.80
long	16.00
dma	
pmsa	
asnum	25528
asnum	2108
throughput	vhigh
proxy	anonymous

EdgeScape information	
ip	161.53.74.122
country_code	HR
region_code	
county	
city	ZAGREB
zip	
timezone	GMT+1
areacode	
georegion	
network	
network_type	
company	Fakultet_elektrotehnike_i_racunarstva
domain	kset.org
fips	
lat	
long	
dma	
pmsa	
asnum	25528
asnum	2108
throughput	vhigh
proxy	anonymous

While both IPs used an anonymous proxy, both used identical HTTP headers and attack payloads – making it highly probable that both are the same person or organization



**Akamai**

Source: Akamai CSI

RSA Conference 2015



# Spain vs. Netherland

13 JUN 2014 - 16:00 Local time  
GROUP B  
Arena Fonte Nova  
Salvador

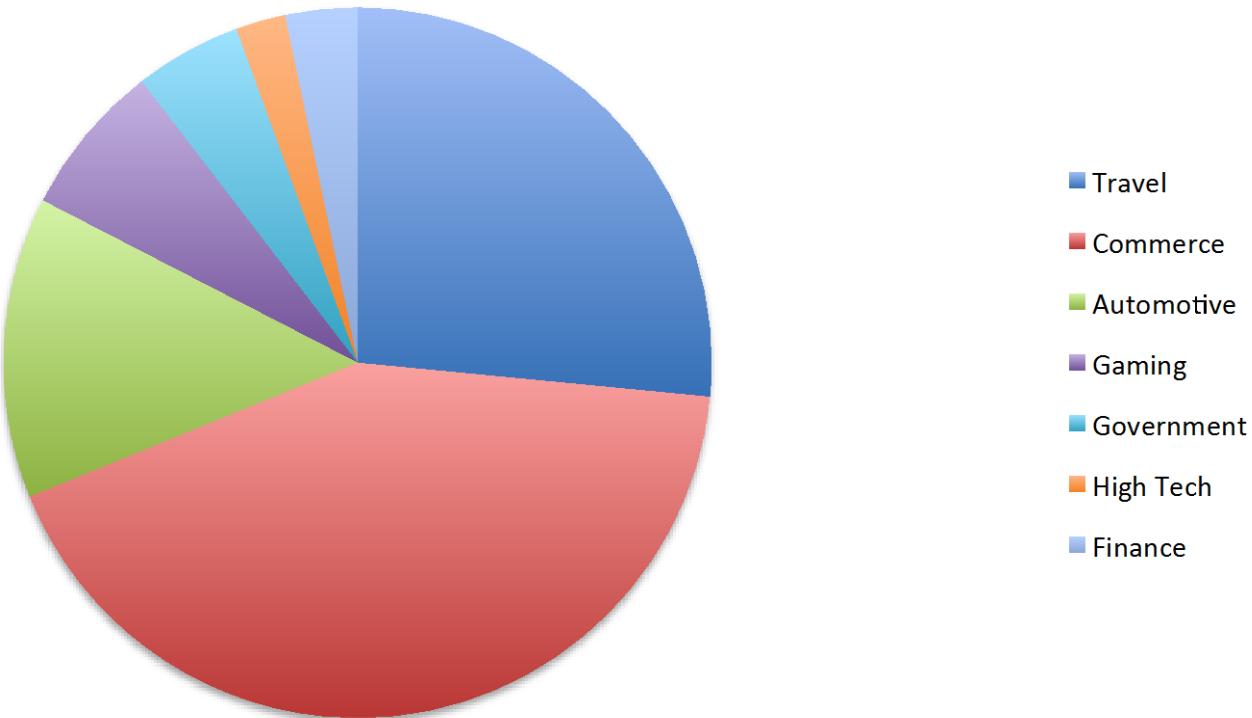
SPAIN

FULL-TIME  
1-5

NETHERLANDS

- Spanish hacker decides to retaliate with an App-layer DoS attack, targeting a major Dutch media/news site Referring page for the attack →
- Most attacks came from a single IP (no proxy used): 80.244.\*.\*
- Target page was /ad/article/detail/live/introduction.do with 98% of the hits – a total of 232,498
- All 232,498 request were identical
- Looking at the HTTP headers – it's obvious the attacker knew exactly what he/she was doing - they created an HTTP request that included: cookies, valid browser headers (mimic a real browser), including “X-Requested-With: XMLHttpRequest” to mimic an AJAX request. Only “flaw” was that session cookies never refreshed throughout the entire attack

# SQL Injection: Top 50 customers attacked by volume



# SQL Injection Analysis of 2000 customers over one week

## Protocol Breakdown

	SQL Injection Attacks	%
HTTP	8,137,681	96.6
HTTPS	287,808	3.4
<b>Total</b>	<b>8,425,489</b>	<b>100</b>

## Breakdown by Intent

Malicious Intention	Malicious Transactions	%
Login bypass & privilege escalation	5,467	0.0649
Data Corruption	2,238	0.0266
Content Injection	8,156	0.0968
Remote Command Execution	794	0.0094
Environment probing & recon.	1,306,681	15.5087
Credential Theft	1,950,749	23.1529
Database content retrieval	129,814	1.5407
SQL Injection Probing	5,021,240	59.5958
File Exfiltration	24	0.0003
Denial of Service	326	0.0039
<b>Total</b>	<b>8,425,489</b>	<b>100</b>

## SQL Injection Breakdown: SQL injection probing

- This step represents 60% of SQLi Traffic
- As a first step, attackers will usually perform an assessment of the web application to see if it is vulnerable to SQL Injection.
- Sample payloads include: sequences of SQL-sensitive characters like:
  - apostrophe ('),
  - semicolon (;)
- Modern approaches use Blind SQL injection techniques such as forming Boolean conditions - AND 1=1, AND 1=0, as well as “timed attacks” such as those using the WAITFOR or sleep() functions.

# SQL Injection Breakdown: Environment probing & reconnaissance

- Makes up 16% of SQL Injection Traffic
- After the attacker concludes that the application is vulnerable to SQL Injection, he/she will take the attack a step further, by trying to learn the type & structure of the database, its tables, columns, users and permissions.
- Common Payload Example:
  - Extraction of information from the MySQL INFORMATION\_SCHEMA table, for example: UNION SELECT group\_concat(COLUMN\_NAME) FROM INFORMATION\_SCHEMA.COLUMNS—

# SQL Injection Breakdown: Credential Theft

- 23% of SQL Injection traffic
- Attempts to steal user credentials through SQL Injection
- These attacks included attempts to retrieve data from tables and views such as:
  - mysql.user (Mysql)
  - master.syslogins (MS-SQL)
  - master.dbo.sysxlogins (MS-SQL)
  - ALL\_USERS (Oracle)

# SQL Injection Breakdown: Database Content Retrieval

- Makes up 1.5% of SQL Injection Attack Traffic
- Once the attacker has a clear understanding of the type and structure of the database and its tables, he/she can start retrieving contents remotely by using several techniques such as data extraction using UNION SELECT statements, or by using Blind SQL Injection techniques (using Boolean expressions).

# SQL Injection Breakdown:

## Login Bypass and Privilege Escalation

- Makes up .06% of SQL Injection Traffic
- The Majority of Web Apps use a SQL back end to check user credentials
- This provides hackers with a simple yet extremely effective method of bypassing the login mechanism using SQL Injection attacks.
- Sample Payload
  - ' OR 1=1-- as the user name.
  - In cases where the hacker knows the user name of the administrator (e.g. "admin"), he/she could attempt to elevate their privileges by logging in with the user name: admin' or 1=1--

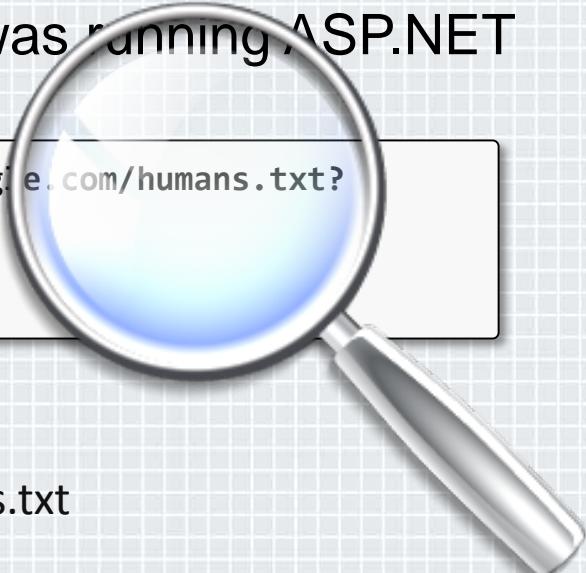
# SQL Injection Breakdown: Denial of Service

- 0.0039% of the malicious requests were classified as attempts to deny service from other users by either overloading or shutting down the database server.
- The most observed vectors were:
  - Excessive use of timed queries with extremely high value of time intervals
  - Attempts to use the MS-SQL SHUTDOWN management command

# Application Scanning

An attempt to exploit an old (2007) WordPress Remote File Inclusion vulnerability. The victim application was running ASP.NET

```
GET /wp-content/wordtube-button.php?wpPATH=http://www.google.com/humans.txt?  
HTTP/1.1  
Host: www.vulnerable.site  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4)
```



Attacked parameter : wpPATH

Malicious payload: http://www.google.com/humans.txt

# What Else Did This Attacker Do On This Site?

Same attacker Sent 2122 different RFI exploit attempts



# Was There Similar Activity Going On At The Same Time?

Attacks originated from a botnet containing **272** attacking machines

**1696** victim applications were targeted

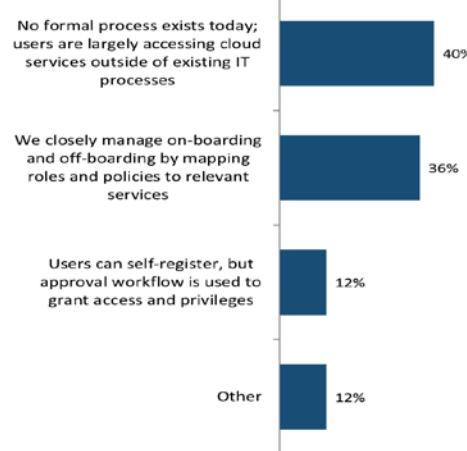
**1,358,980** attacks were launched during the campaign

The campaign lasted for **2** weeks

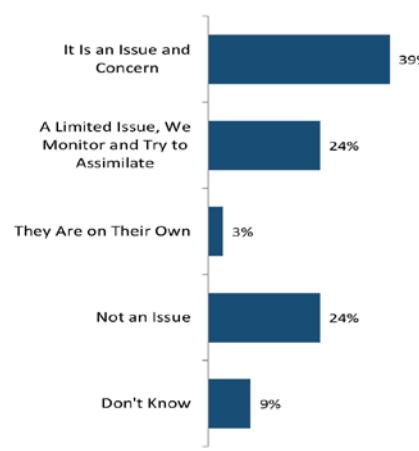
# Shadow IT: “It’s pretty loose today”

## On-boarding External Cloud Services

### On-board, External Cloud Access



### Impact of No Formal Process



Left Chart, Q. Which of the following best describes your existing approach to on-boarding users who need access to external cloud-based services? n=83; Right Chart, Q. If no formal process exists and ‘shadow IT’ is an issue, please describe the impact that has on your organization. n=83.

Source: Cloud – Wave 6 | © 2014 451 Research, LLC [www.451research.com](http://www.451research.com)

“People can sign up to Amazon or Azure, create user credentials to do it and spin stuff up. That hasn’t been completely reeled in yet. We want an internal group that brokers cloud services. Establishes guidelines and preferred providers they would leverage and anything else around that. It’s pretty loose today.” – LE, Financial Services

# Implications of Shadow IT growing so quickly

## Traditional IT

- Full lifecycle costs are considered
  - Application Creation
  - Software Patching
  - Auditing/Scanning
  - Vulnerability remediation
  - Application Decommissioning

## Shadow IT

- Fast, Cheap, and Easy
  - Software Patching?
  - Scanning?
  - Application End of Life?

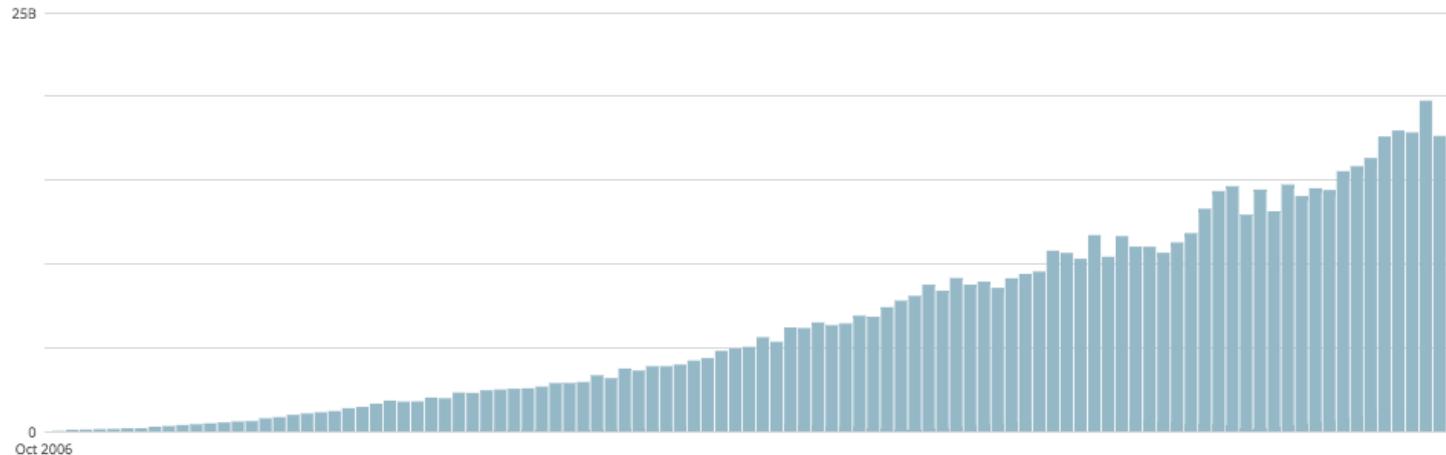
# Easy-to-use CMS's Power Shadow IT

## ~ 20% of sites on the Web use WordPress

### Traffic WordPress.com

#### Views

The number of pageviews across blogs we host here on WordPress.com, both on subdomains and their own domains, or externally-hosted blogs that use [our Jetpack plugin](#) and are part of our network.



Akamai

Source: Wordpress.com

RSA Conference 2015

# CMS Plugins: Summary of 1 day's Attack Traffic



**SLIDER REVOLUTION**  
A PREMIUM WORDPRESS PLUGIN

- » **Responsive** with any dimension, Full-Width, Fullscreen
- » Huge Feature Update! [SEE FILE DESCRIPTION](#)
- » Now with Loop Animations & Parallax Layers
- » Multi-Language Ready with WPML or QTranslate
- » **Brand-New Backend Functionality & Style**
- » The Plugin of Choice for many Theme Authors!

VERSION 4.6  
SkyWood

responsive sales

WPML CSS Android Vimeo YouTube

1134 customers probed  
Source IP's:17



Wordpress FileManager

Index of /wp-content/

Name	Rn	Rm	Name	Size	Vw	Ed	Rn	Dl	Rm
index.php			index.html	395 B					
license.txt			readme.html	19,46 kB					
test_create			wp-activate.php	8,96 kB					
wp-admin			wp-blog-header.php	4,35 kB					
wp-content			wp-comments-post.php	271 B					
wp-includes			wp-config-sample.php	3,44 kB					
			wp-config.php	3,10 kB					
			wp-cron.php	3,36 kB					
			wp-links-opml.php	2,65 kB					
			wp-load.php	1,95 kB					
				2,35 kB					

1028 customers probed  
Source IP's:107



APPS. FOR SMALL BUSINESSES WITH BIG IDEAS.

Zingiri Web Shop

zingiri

963 customers probed  
Source IP's: 7



Salutation

Styles Features Blog Portfolio BuddyPress Shortcodes Contact Sign In

711 customers probed  
Source IP's:42



SHOWBIZ<sup>PRO</sup>

Premium jQuery plugin

Showbiz Pro is a responsive plugin that allows you to show front content with a set amount of teaser items. The size and amount of teaser items will automatically adjust depending on the browser size. Check out the Preview below to grasp the full potential of Showbiz Pro.

653 customers probed  
Source IP's:19

# `#!/bin/bash_`

```
~root: env X=""() { :;}; echo shellshock" /bin/sh -c "echo completed"  
> shellshock  
> completed
```

120,000+

## UNIQUE ATTACK PAYLOADS

Exploit  
Announced



9/24

9/25

9/26

9/27

9/28

9/29

9/30

10/1



# Shellshock/Bash Probing: One week's summary

Country	Total Triggers	Source IPs
US	146272	273
GB	96816	50
FR	29791	19
DE	28416	31
JP	27790	12
KR	26447	7
UA	23510	2
AT	21192	1
CN	16038	81
IT	5830	5
GR	3830	4
CZ	3738	4
CA	1711	7
PL	937	1
NL	881	22
AU	605	4
IN	575	15
BR	422	14

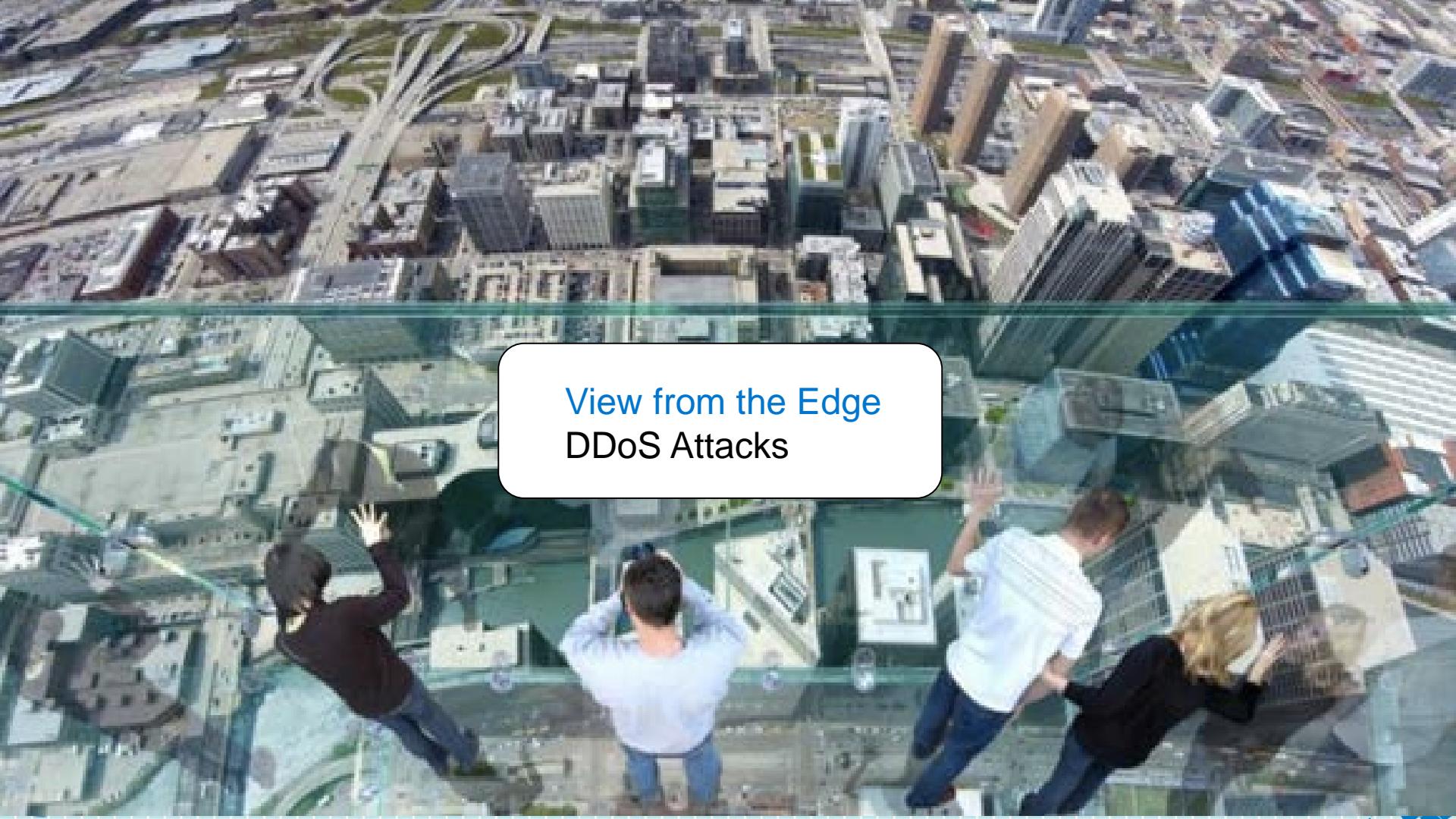
Vertical	Num. Attacks
Media & Entertainment	150325
Software as a Service	96222
Business Services	45586
High Technology	39586
Retail	36461
Hotel & Travel	24429
Financial Services	22412
Consumer Goods	10194
Real Estate	4188
Gaming	2501
Public Sector	1387
Foundation-Not for Profit	1027
Pharma/Health Care	567
Energy & Utilities	566
Manufacturing	498
Consumer Services	433
Automotive	189
Education	8

**Total source attacking IPs: 656**

**Total targeted customers: 2,570**

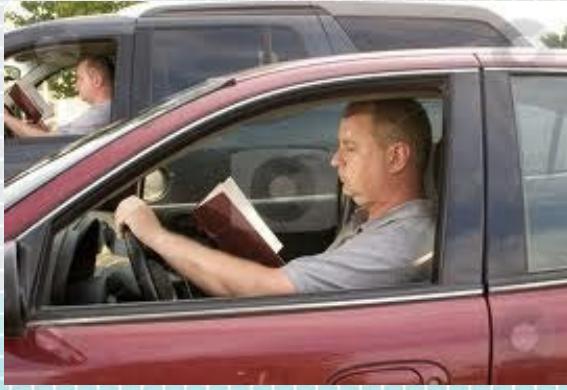
**Total attack transactions: 436,641**





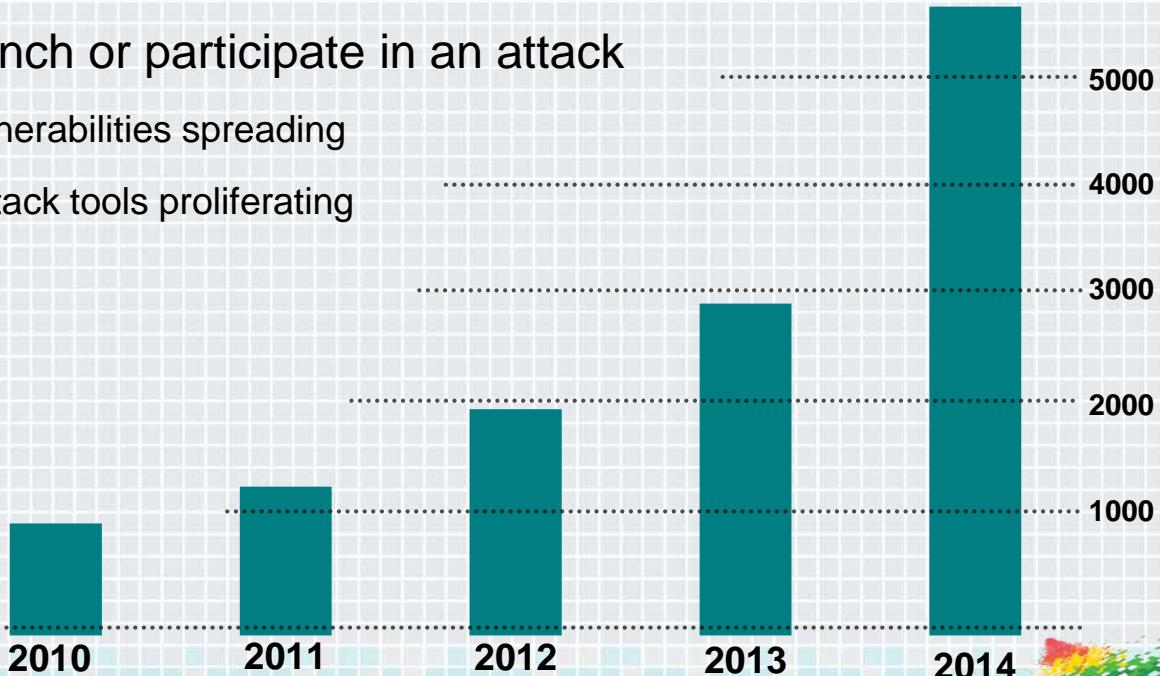
View from the Edge  
DDoS Attacks

# Even if your Security Practice is Perfect: You share the Internet with others



# Frequency of DDoS Attacks Continues to Increase

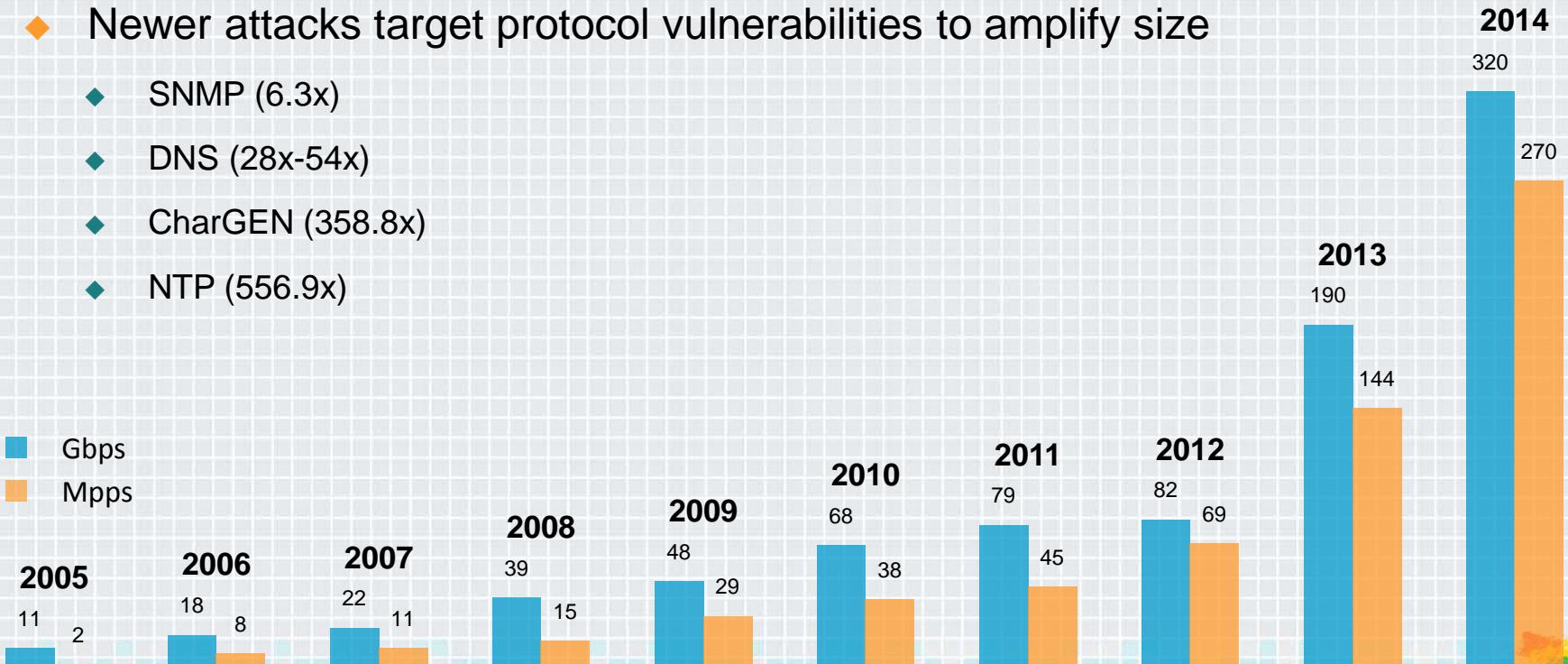
- ◆ Increasing number of network- and application-layer attacks
- ◆ Easier for attackers to launch or participate in an attack
  - ◆ Knowledge of application vulnerabilities spreading
  - ◆ Number and availability of attack tools proliferating



# DDoS Attacks Are Growing in Size

- ◆ Newer attacks target protocol vulnerabilities to amplify size

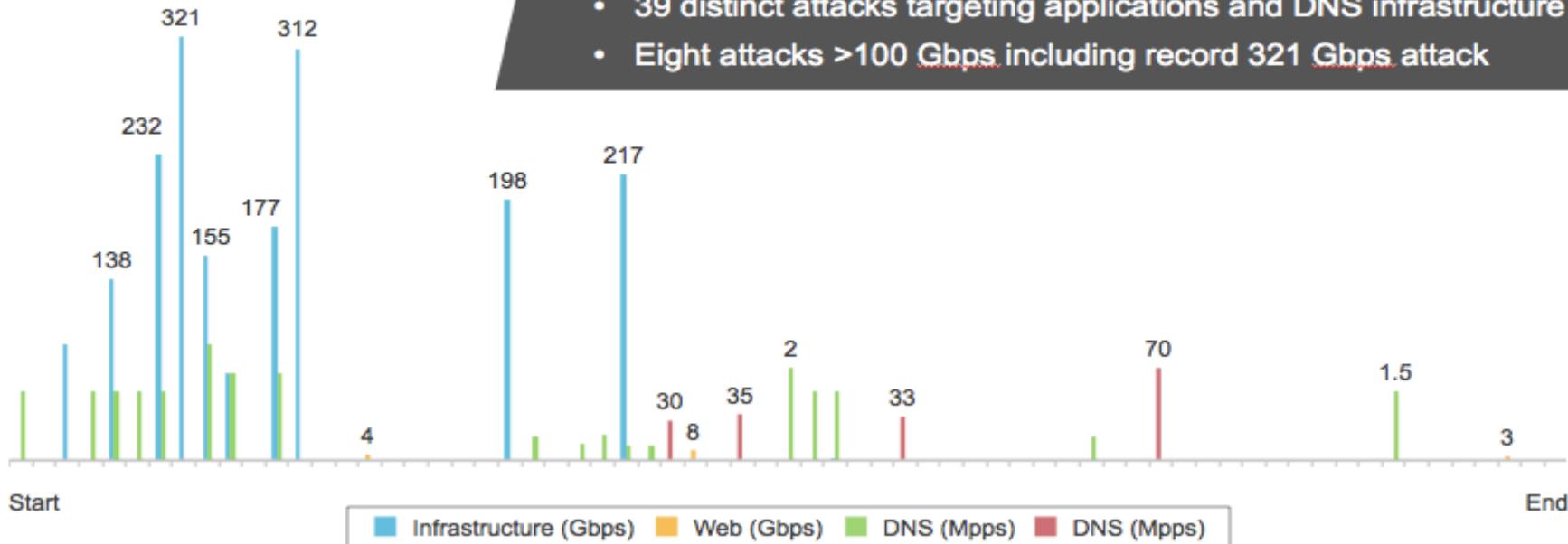
- ◆ SNMP (6.3x)
- ◆ DNS (28x-54x)
- ◆ CharGEN (358.8x)
- ◆ NTP (556.9x)



# Multi-Vector Attacks are the Norm

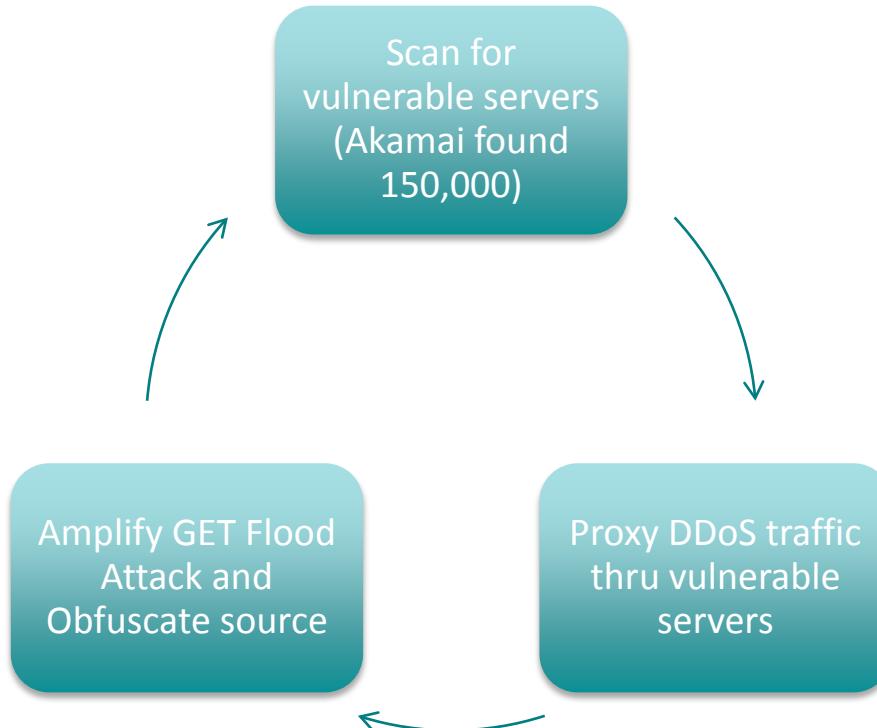
## Two-month campaign against single customer

- 39 distinct attacks targeting applications and DNS infrastructure
- Eight attacks >100 Gbps including record 321 Gbps attack



# Vulnerability in Google Maps plugin for Joomla enables DDoS attacks

#RSAC



# Tools such as DavoSet/UFONet are leveraging the Proxy Vulnerability

#RSAC

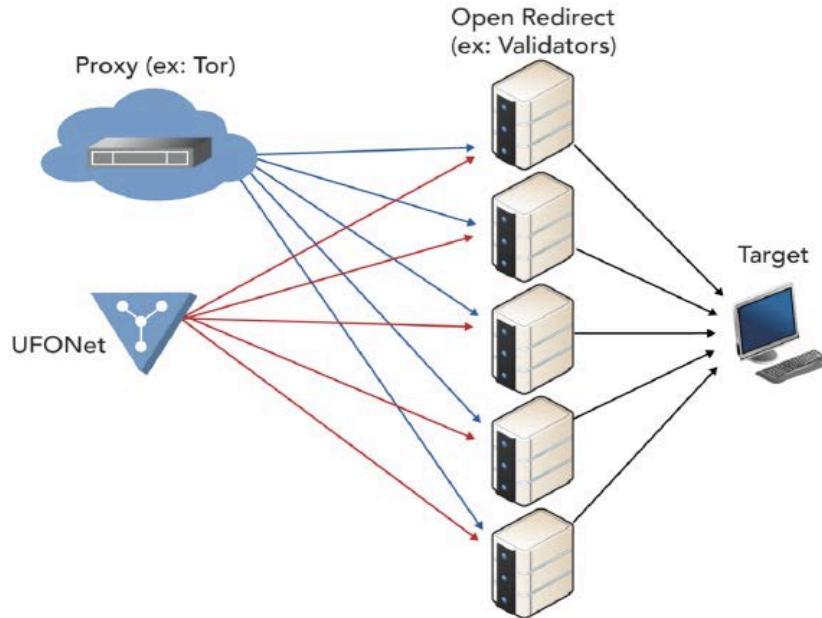


Figure 2: How a UFONet attack works with a proxy (SourceForge)

# UFONet UI

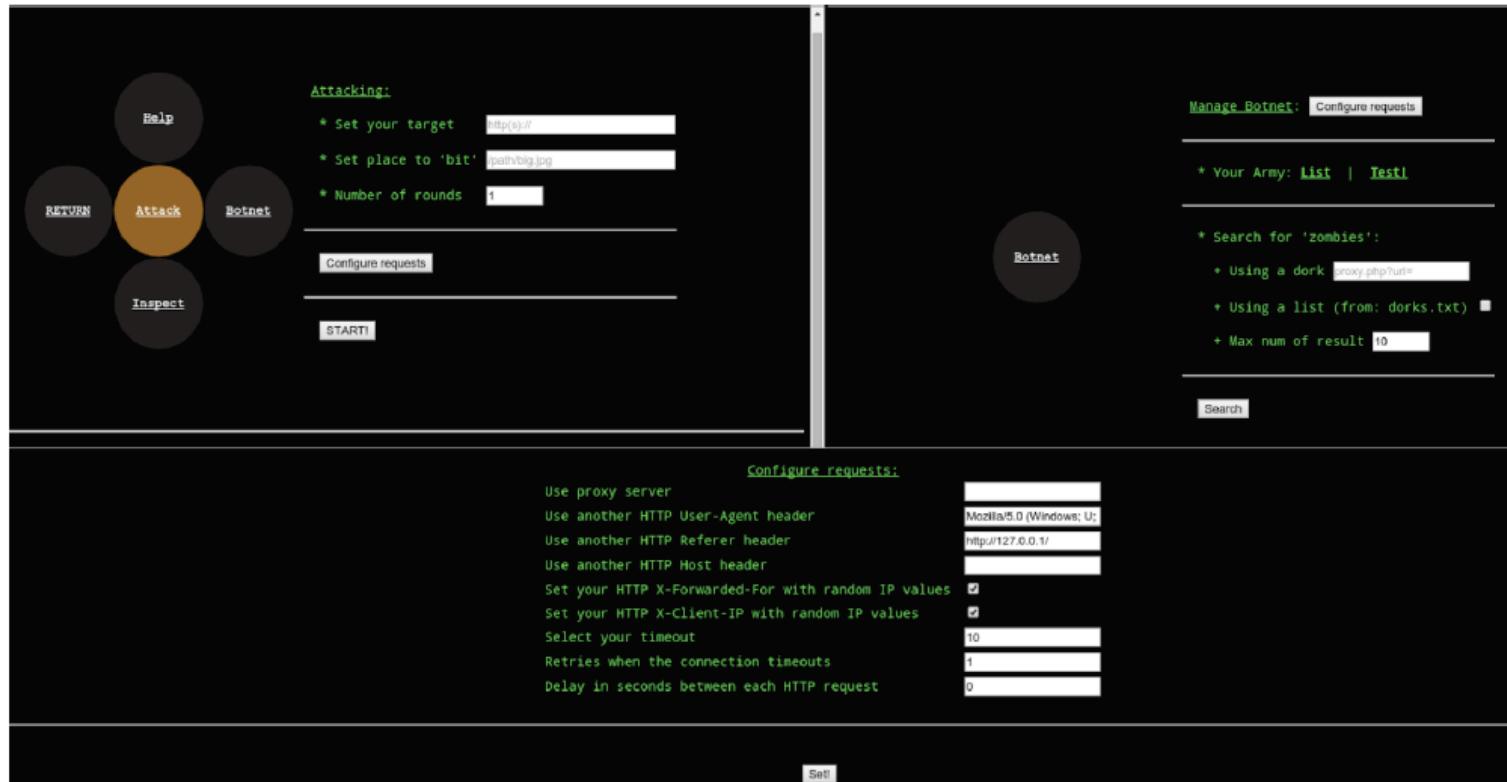


Figure 3: The UFONet web interface allows users to quickly configure and launch DDoS attacks

# Joomla GET Flood DDoS Attacks

## Bandwidth and Vector Combination per Attack

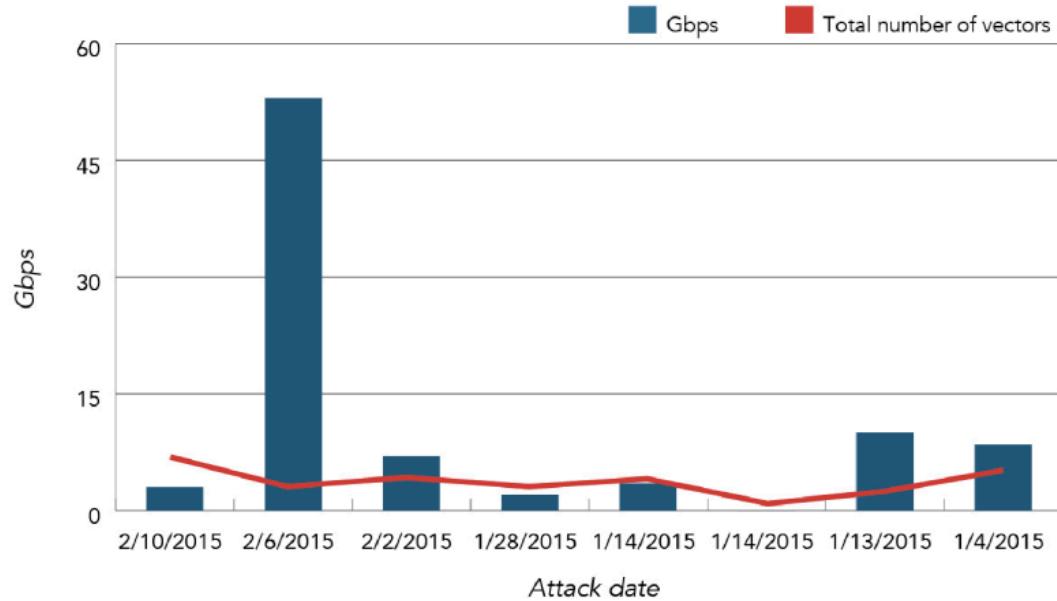


Figure 7: Dates, peak bandwidth and total vectors per attack

# Account Checkers as a service

Delim: |  Hide result die  Check MP Live

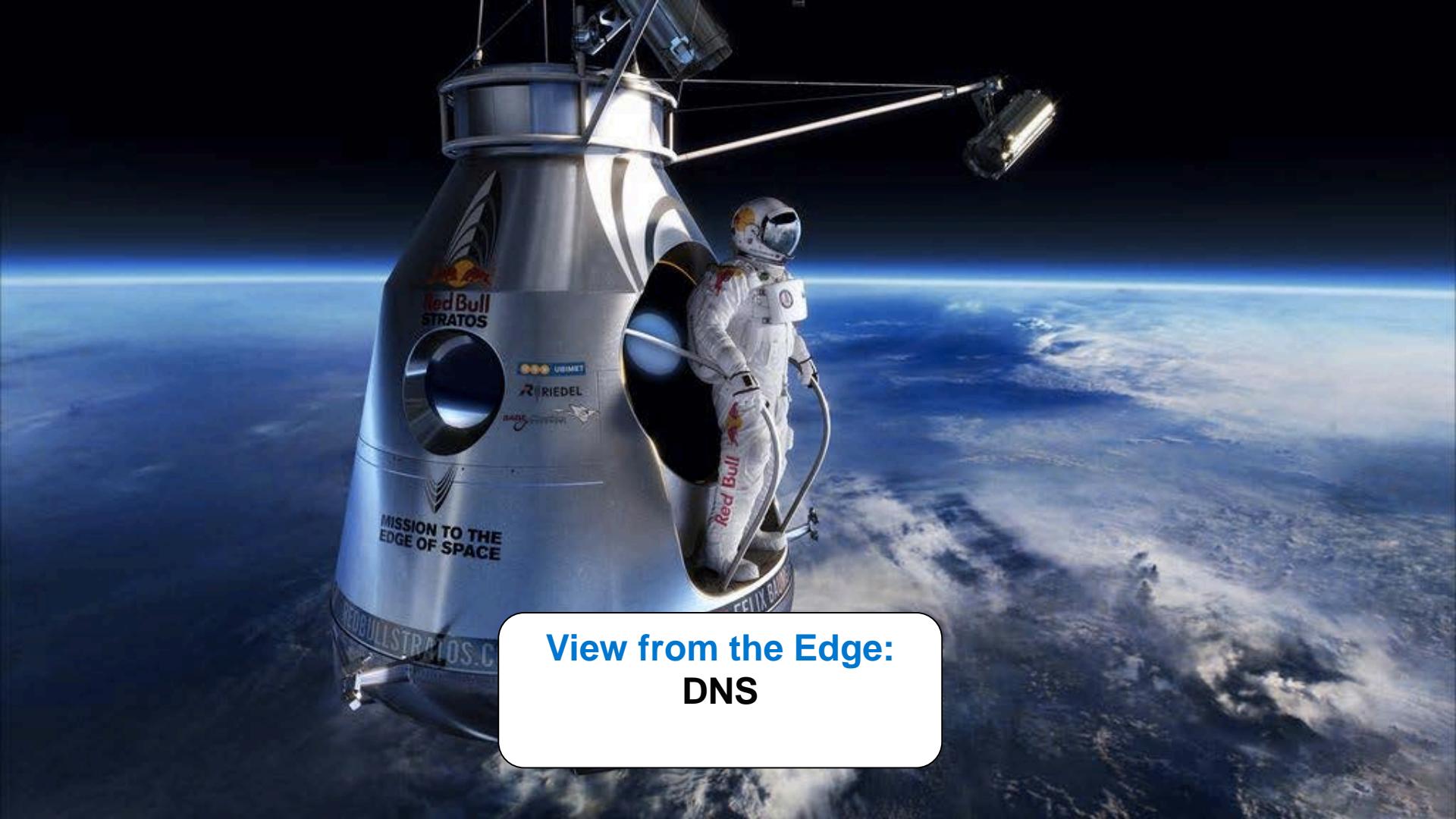
CHECK NOW

- ▼ Choicehotels
- Coldwatercreek
- Thelimited
- Bonton
- Bergdorfgoodman
- Bestbuy
- Bloomingdales
- BN
- Bjs
- Cabelas
- Choicehotels**
- Costco
- Clubcarlson
- Datafile
- Dell
- Lanebryant
- Avenue
- Drugstore
- Bestwestern
- Dillards
- Ebay

# Account Checking Tool - Internals

## After Credential Matching: Script to Match on Credit Card in Account

```
preg_match_all( '/name="([^\"]+creditCardId)"[^>]*value="([^\"]+)" /si' , $page, $matches);  
  
$cardIDs = $matches[2];  
  
$ccCount = count($cardIDs);  
  
  
foreach ($cardIDs as $cid)  
{  
  
    $url = "https://m.<site>.com/account/wallet";  
  
    $post = 'action=EDIT&creditCardVB.creditCardId=' . $cid . '&validationCheck=false';  
  
    $page = $curl->post($url, $post, 1, 1, 0);
```



**View from the Edge:  
DNS**

# DNS Hijacks

You lock your car



You lock your home



You should lock your DNS



# Best Practice DNS Locks

## Client DNS Locks

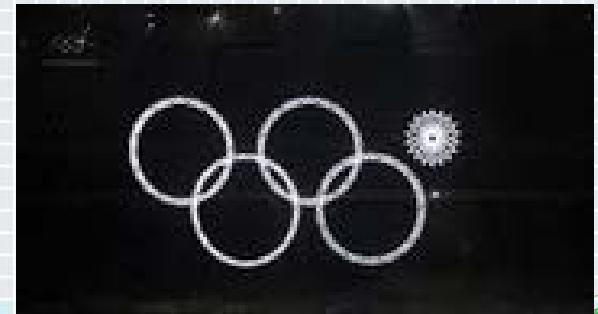
- clientUpdateProhibited
- clientTransferProhibited
- clientDeleteProhibited

## Registrar locks

- serverUpdateProhibited
- serverTransferProhibited
- serverDeleteProhibited

# Multi-Vector Attacks: 2014 Sochi Olympics

- **3.5 Tbps event**
  - 50% Growth in Average User Connection Speed Compared to 2012.
  - More than a Million Malicious Requests Blocked
- **Multi-Vector Attacks Detected Again in 2014**
  - Application DDoS
  - RFI
  - Command Injection
  - Requests from Anonymous Proxy
- **Attacks Again Spiked During Major Events**
  - Opening Ceremonies
  - Hockey Semi-Final(US v. Canada)



# Summary

- Web Applications are under constant scanning for vulnerabilities
- How long do you have to patch a new vulnerability like ShellShock?
  - Hours, up to a week if you are really lucky
- DDoS Attacks continue to increase in complexity and scale
  - Driven by servers commandeered by Web Application Vulnerabilities
  - Also driven by reflection attacks
- Please lock your DNS at your registrar
- Multi-Vector Attacks are the norm

# Security Basics

Start Time	Title	Presenter
8:30 AM	Introduction	Hugh Thompson
8:45 AM	Security Industry and Trends	Hugh Thompson
9:30 AM	User Authentication Trends and Methods for Native Mobile Applications	Kayvan Alikhani
10:15 AM	BREAK	
10:30 AM	Mobile & IOT Security: Will Big Data Make it Better or Worse?	Hadi Nahari
11:15 AM	Viruses, Malware and Threats	Tas Giakouminakis
12:00 PM	LUNCH	
1:15 PM	Crypto 101: Encryption, Codebreaking, SSL, and Bitcoin	Benjamin Jun
2:00 PM	Security Enforcement Explained	Dana Wolf
2:45 PM	BREAK	
3:00 PM	Internet and Web Security Issues	Patrick Sullivan
3:45 PM	Network Security	Gary Sockrider

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: SEM-M01

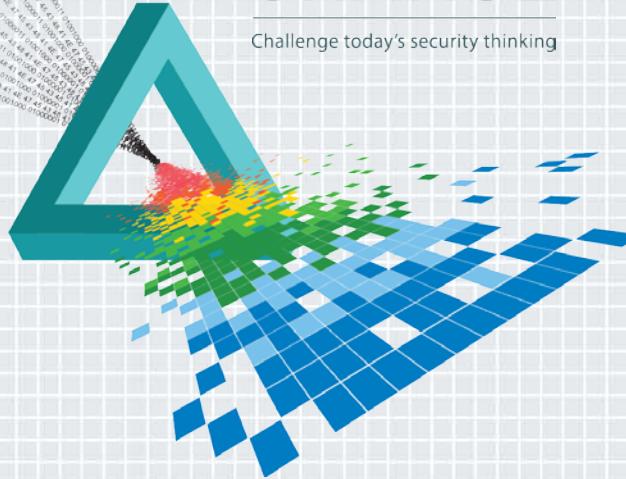
## Network Security 101

Gary Sockrider

Solutions Architect  
Arbor Networks  
[@arbornetworks](https://twitter.com/arbornetworks)

# CHANGE

Challenge today's security thinking



# Last Session of the Day!



# What to Expect from this Session

- ◆ No “Death by Powerpoint”
- ◆ Interactive Discussion
- ◆ Audience Participation
- ◆ Learn Something!

# What is Network Security?

- ◆ What is most important?
- ◆ Define your network?
- ◆ Where do I start?
- ◆ Who is in control?

# The Global Network is Your Business

Diverse end-points are accessing your network from anywhere.



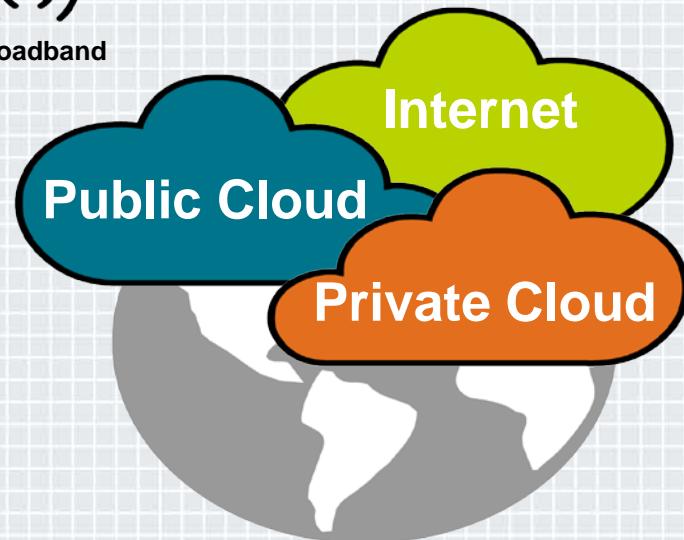
Corporate Offices



Mobile



Broadband



Internet

Public Cloud

Private Cloud

Your assets are distributed everywhere.



Content



SaaS



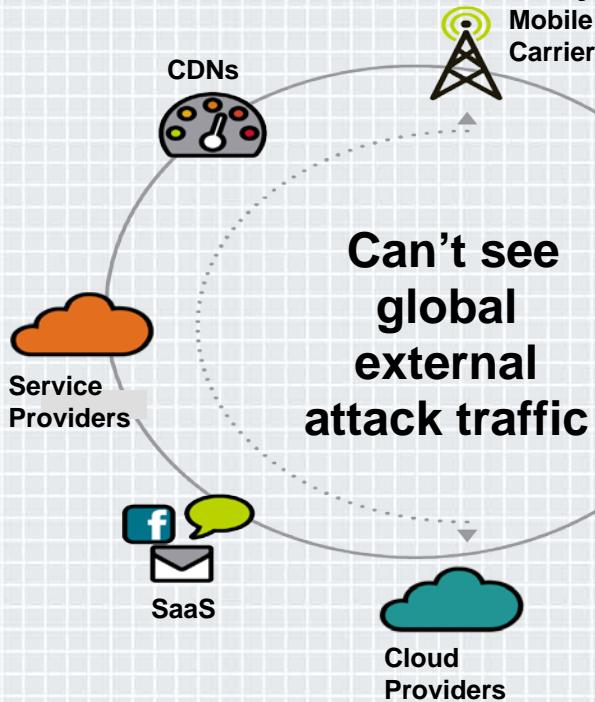
Corporate Servers & Applications

# Network Perimeter Security

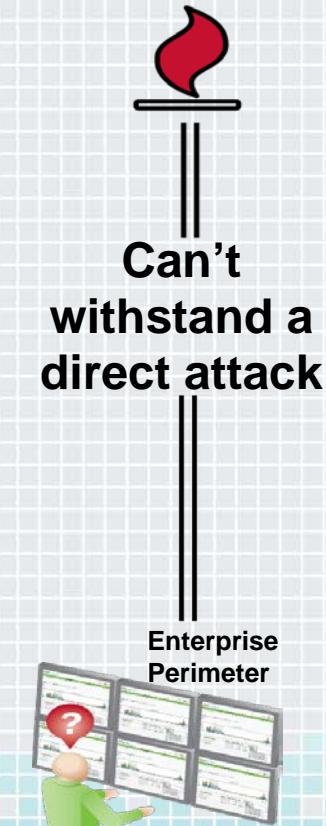


# Problem Fueling \$1Billion+ In Security Spend

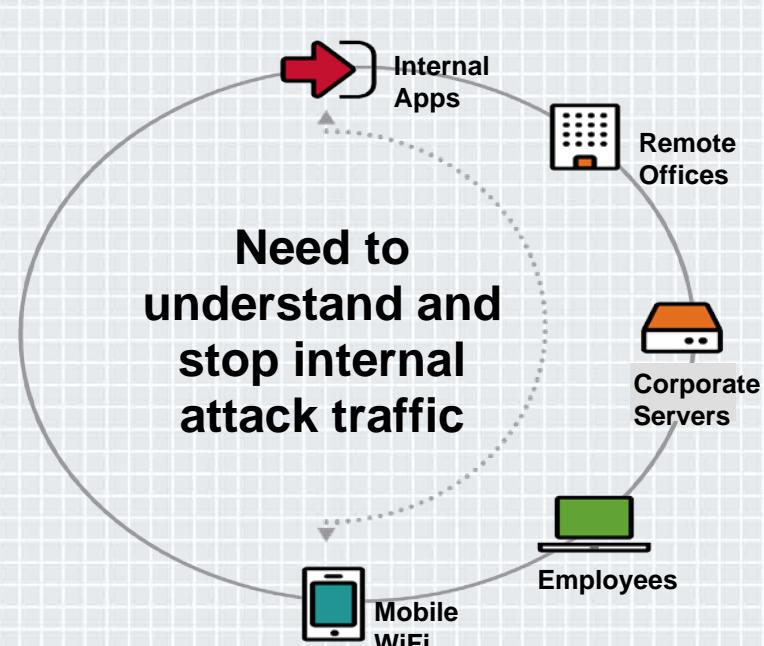
## Global Traffic Visibility



## Availability Protection

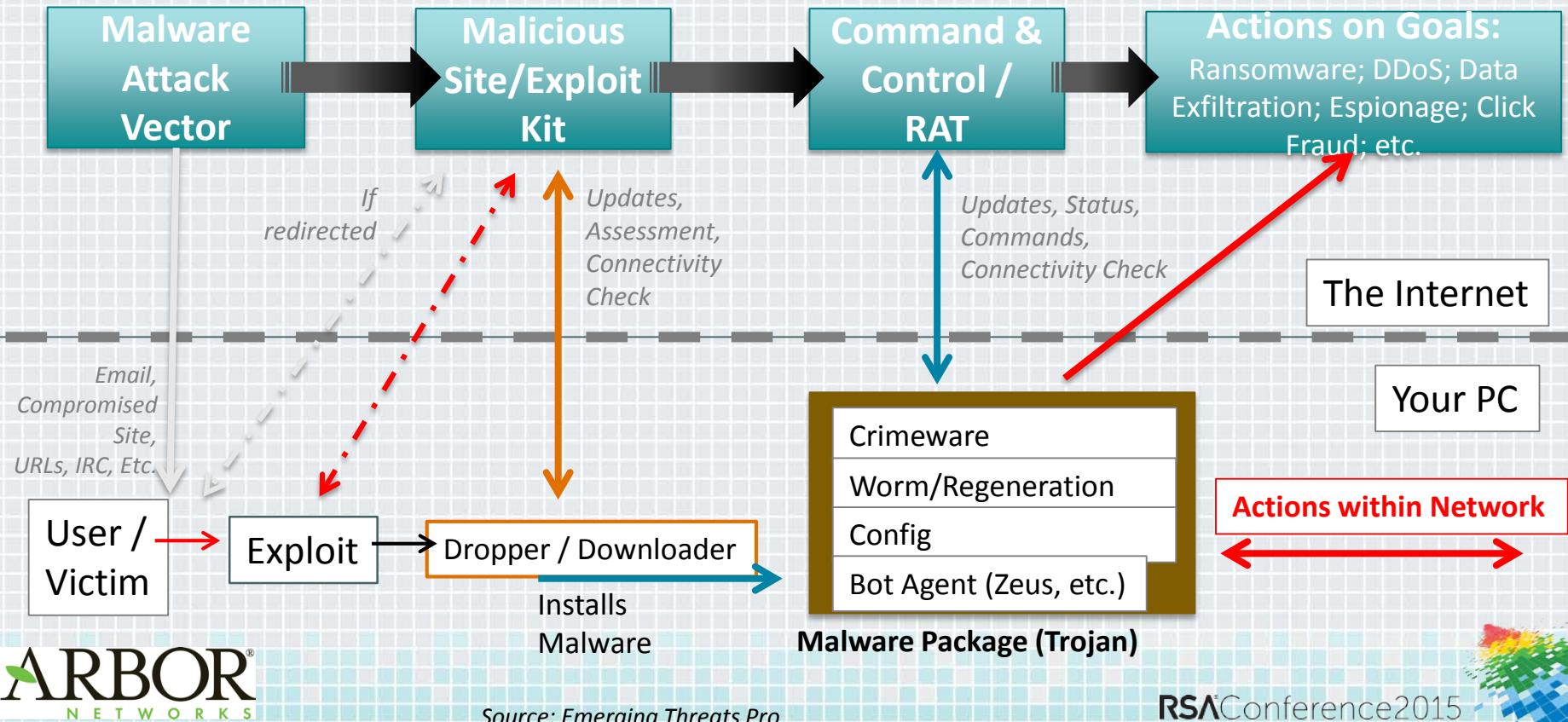


## Internal Traffic Visibility



# Malware Is An *Ecosystem*, Not Just a Sample or Simple Signature

#RSAC

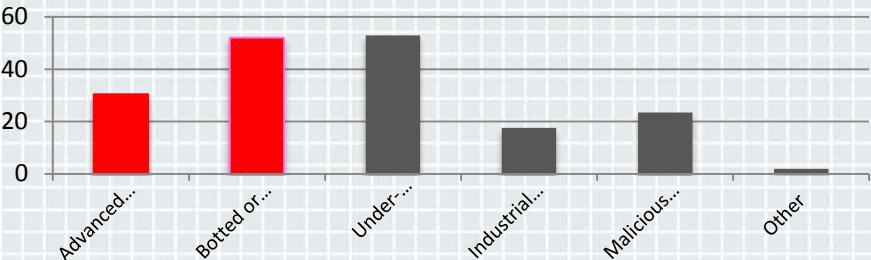


# How are threats getting through?



- Huge number of ‘ways in’
  - Drive By Download
  - SPAM/Phishing
  - Watering Hole
  - USB
- Many threat vectors
  - New AND Old
  - IPS / AV Limited coverage
  - Patching lag
- Leverage vulnerabilities
  - Zero Day
  - Java, Adobe, etc.
  - Compound Documents

Threats On Corporate Network



# So, how do we get ‘better’ at this?

- **Actionable Threat Intelligence**
  - Use the expertise within vendors, integrators to maximize your effectiveness
- **Broad Visibility**
  - Monitor within your network, not just at the perimeter
- **Deep Visibility & Context**
  - Full packet capture and threat detection at key network locations
- **Improved Workflow**
  - Invest in solutions that fit into an Incident Response workflow and enable personnel and processes



# Actionable Threat Intelligence

Threat intelligence is a top priority for 75% of firms

"Which of the following initiatives are likely to be your firm's/organization's top IT security priorities over the next 12 months?"  
(Establish/tuners threat intelligence capabilities)



COMPUTER CRIMES



# Broad Visibility - Flow

Leverage Flow technologies for

- ◆ Cost-effective, scalable visibility
- ◆ Layer 3/4 picture of internal network

Understand who talks to who, when and how much

- ◆ Develop a model of normal network / user behavior
- ◆ Build policy/visibility around user-identity

Correlate with ***actionable threat intelligence***

Detect suspicious or malicious activities wherever they occur

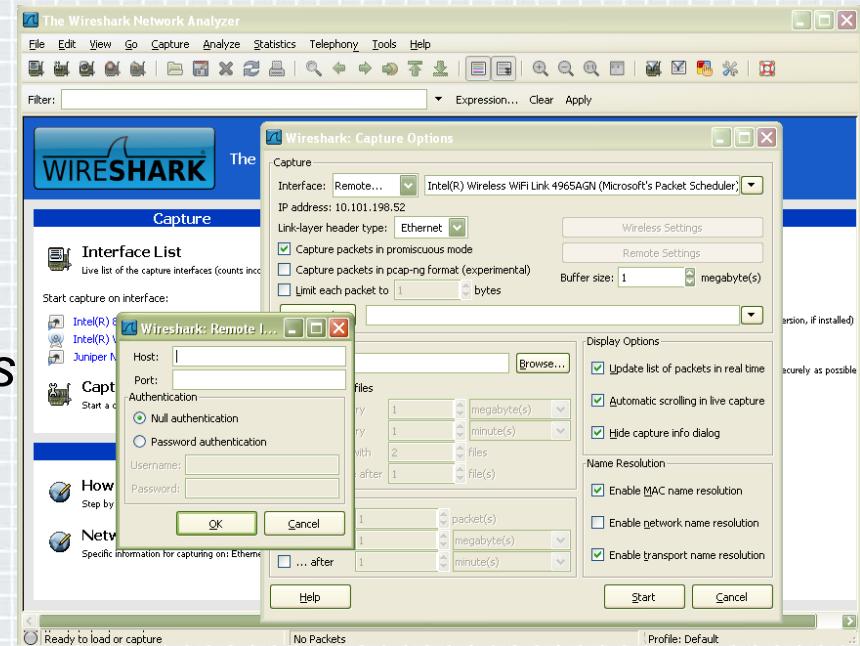


# Deep Visibility & Context – Packet Capture

Use high-speed packet capture for deeper visibility

- ◆ Monitor for specific threats at network / data-centre edge(s)
- ◆ Full-fidelity storage of forensic data *for interactive, retrospective analysis*
- ◆ Investigate scope of compromise / kill chain

Correlate (continuously)



# Improved Workflow

Put the power back in the hands of the analysts

- ◆ Network & Threat Visibility, *in context*
- ◆ Improve the Incident Response workflow
  - ◆ Make drastic improvements to Detection/Analysis
  - ◆ Enhance Containment, Eradication and Recovery timelines

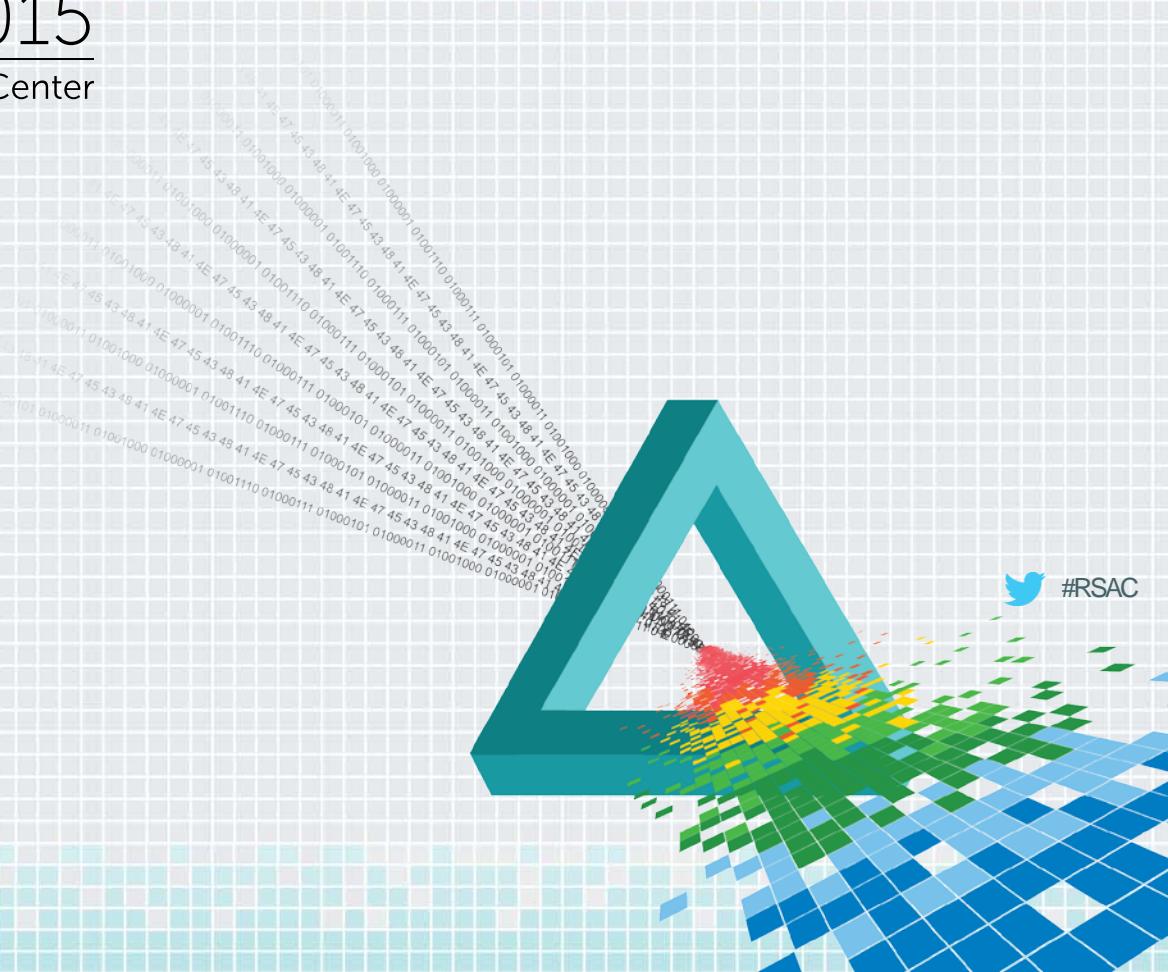
Technology should **enable** personnel & process investment

- ◆ Regardless of how many you have or skillset

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

## What Now?



# How to apply what you have learned

- ◆ Understanding
  - ◆ Identify Knowledge Gaps
  - ◆ Plan for the Future
  - ◆ Collaborate with Colleagues
- ◆ Continuous Development
  - ◆ Keep Asking Questions
  - ◆ Join a Network or Security Organization
  - ◆ Participate/Sponsor War Games

# Questions?

Gary Sockrider

Arbor Networks

[sock@arbor.net](mailto:sock@arbor.net)

@arbornetworks