CINC UP: CYBERSECURITY RESEARCH ACCELERATION WORKSHOP AND SHOWCASE

Brought to you by CENIC and Internet2

JOHN DUNDAS
VP and CTO, CENIC

FLORENCE HUDSON
SVP & Chief Innovation Officer, Internet2

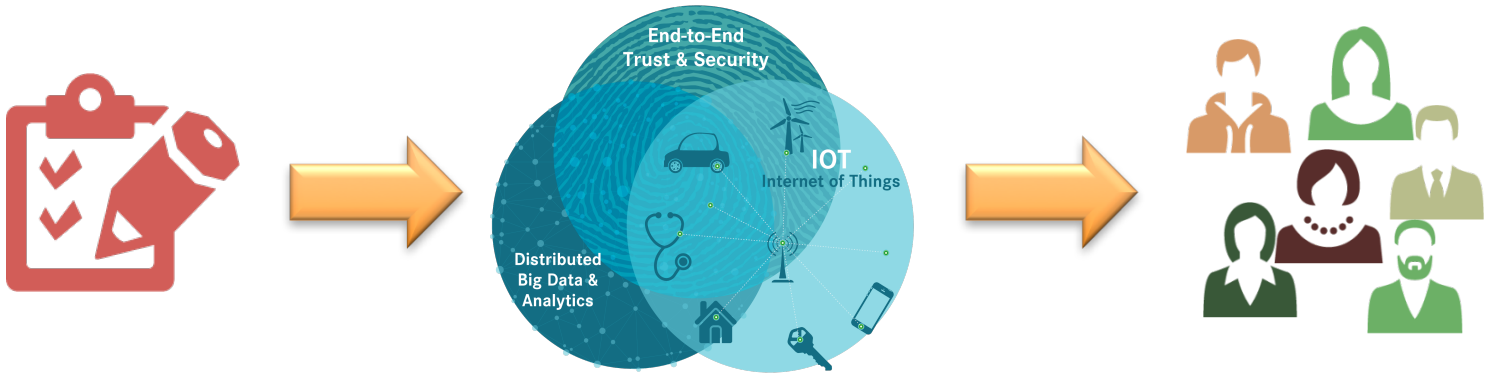
CINC UP: CYBERSECURITY RESEARCH ACCELERATION WORKSHOP & SHOWCASE

AGENDA

- Welcome and Introduction
- CIO & Industry Perspective
- NSF Program Director Update
- Cybersecurity Research Panel: Network Security
- Cybersecurity Research Panel: Internet of Things
- Cybersecurity Research Panel: Identity & Access Management
- Cybersecurity Research Panel: Multidisciplinary Cybersecurity

Welcome and Introduction

Internet2 Collaborative Innovation Community was created in 2015 based on a member survey of 8,800 individuals identifying their top areas of interest for open, inclusive, collaborative innovation.



- Three Innovation Working Groups launched at Global Summit in May 2015
- Now, 400+ Collaborative Innovation Community (CINC UP) participants, representing 170+ institutions (as of October 2017)

Internet2 CINC UP combines three member-led innovation working groups, focused on areas brought forward by members, related to our top two priorities of advanced networking plus trust & identity.

E2E Trust & Security (E2ET&S)

- TIPPSS for IoT – Trust, Identity, Privacy, Protection, Safety, Security
- NSF EAGER Cybersecurity Transition to Practice Acceleration
- SDP (Software Defined Perimeter), Network Segmentation for IoT

Distributed Big Data & Analytics (DBDA)

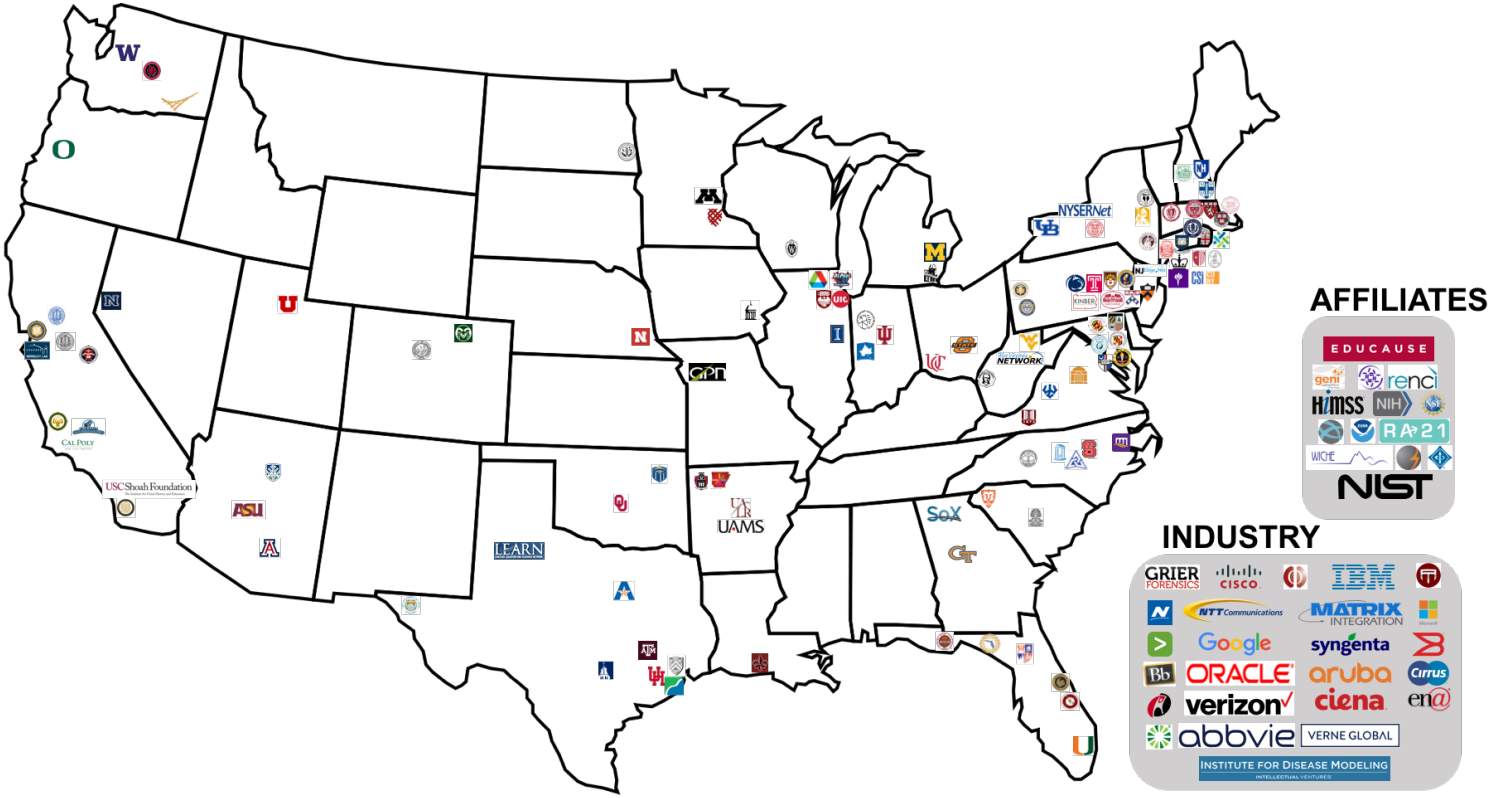
- NSF Big Data Hub Collaboration
- Smart Campuses and Cities
- Health & Life Sciences / Genomics

Internet of Things (IoT)

- IoT Sandbox
- Smart Campuses and Cities
- Smart Grid Testbed

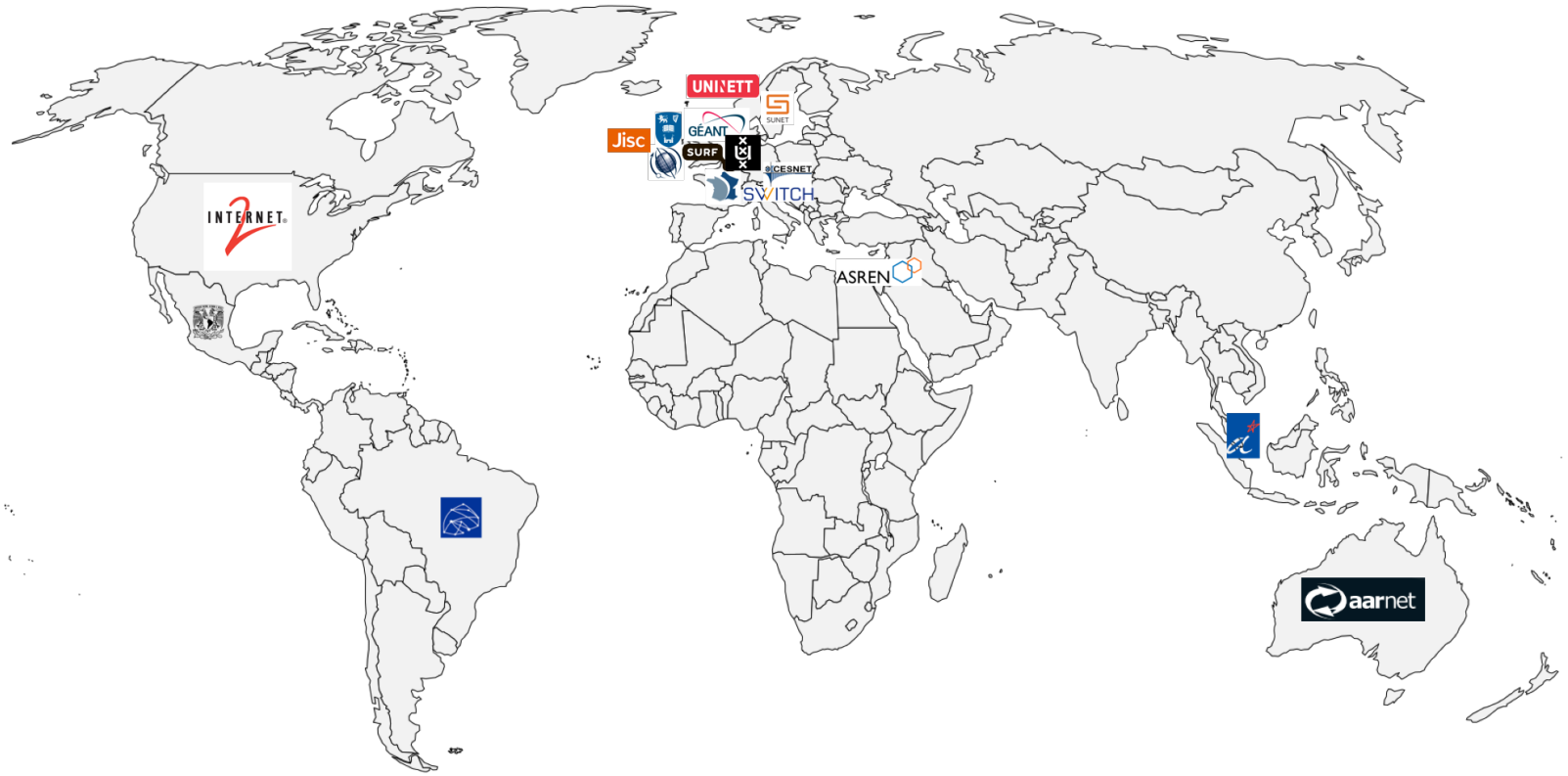
Join us! Email CINO@Internet2.edu

Internet2 CINC UP in the US has grown to 380+ individuals, from 155+ organizations, representing 31% of Internet2 member institutions.



As of October 6, 2017

Globally, the Internet2 Collaborative Innovation Community has grown to 400+ individuals, from 170+ organizations.



As of October 6, 2017

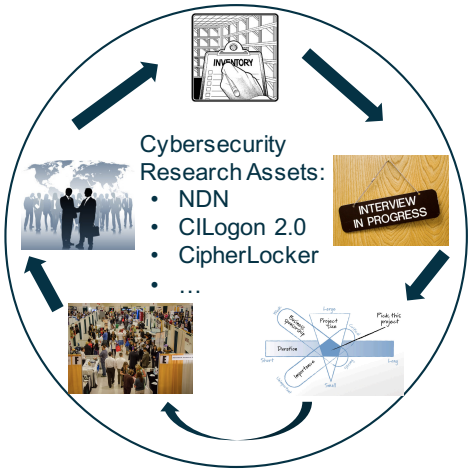
NSF EArly-concept Grant for Exploratory Research (EAGER): Cybersecurity Transition To Practice (TTP) Acceleration

Challenge

- **Accelerate Transition To Practice (TTP)** of NSF-funded later-stage cybersecurity research into **Research & Education environments**

Solution

- Identify & assess NSF cybersecurity research **inventory**
- **Interview** researchers & practitioners for cybersecurity TTP needs, gaps and best practices
- **Leverage Internet2 community** to enable "matchmaking"
- Deploy webinars, portal, in-person **events for researcher/IT matchmaking**
  - San Francisco, Oct 18,12:30-5:30pm



Award Number: 1650445
Internet2
August 2016 – August 2018
PI: Florence Hudson, SVP/Chief Innovation Officer
Team: Emily Nichols, Giselle Trent, Bruce Maas

Scientific Impact

- **Increase awareness** of cybersecurity research & capabilities
- **Accelerate cybersecurity TTP** to make cyberspace safer
- **Identify cybersecurity needs** to inform future research

Broader Impact

- Enable **partnership for NSF TTP with other Federal agency programs** to accelerate & streamline TTP pipeline
- **Enable more diverse R&E pipeline** partnering with Society of Women Engineers and others
- We need you in cybersecurity

SME Interview insights regarding TTP acceleration informed the EAGER project plan

Cybersecurity Researchers

- Key needs for TTP identified: Funding from NSF and others, **early user feedback**
- **User feedback from pilot deployments** critical to accelerate TTP
- Opportunity for acceleration of the TTP process at multiple steps
- Researchers like opportunity to leverage NSF TTP, DHS TTP, I-CORPS **multiple agency support**
- TTP not a priority for some researchers – looking to solve complex problems, not start a business

Practitioners for Pilot Deployments

- Practitioners **need to know operational requirements** for pilot use of TTP assets
- All size universities and regional networks interested in potential to test out / pilot cyber research early
- Smaller universities requested to participate in TTP as they have simpler approval processes
- Some universities unwilling to deploy unproven, non-production tested cybersecurity code

Agencies

- Interested in **cross-agency collaboration** opportunities, e.g., for NSF and DHS, to accelerate cyber TTP

Survey Tools to Collect Feedback

Workshop Overall:
http://bit.ly/ttptechexws

Researcher Assets:
http://bit.ly/ttptechexresearch

NSF Program Director Update

CIO & Industry Perspective

Panelists

Moderator: Bruce Maas, Innovation Fellow, Internet2
Larry Conrad, Associate Vice Chancellor for Information Technology and Chief Information Officer, University of California-Berkeley
Meredith Lee, Executive Director, West Big Data Innovation Hub, University of California-Berkeley
Michael Shepherd, Business Development Manager, Cisco Systems
Ruth Marinshaw, Chief Technology Officer – Research Computing, Stanford University
Bruce Taggart, Vice Provost for Library & Technology Services, Lehigh University

Panel Questions

- **Ruth Marishaw**, you bring the perspective of someone who is already working with faculty researchers in a significant way. And Stanford is already well known for working closely with the private sector. Where do you see opportunities at Stanford related to the TTP goals, and do you have a perspective to share on what kind of approach has worked there in the past?
- **Larry Conrad**, your job is to make sure that every service delivered by Berkeley IT works well all the time. In addition to that primary mission, you are also expected to respond to the needs and interests of a wide diversity of faculty and researchers. How do you envision how your organization could partner with faculty interested in TTP? Can you do this and still fulfill the mission or reliable, dependable services?
- **Meredith Lee,** What are you seeing in the Big Data Hub projects regarding cybersecurity challenges and opportunities? Where do you see some opportunities for researchers to utilize your own campus to advance their research?
- **Bruce Taggart**, you bring the unique experience of someone who is responsible for both library and IT at a research university. Plus, you are already engaged with researchers on your campus. Please discuss how you are collaborating on developing your "Campus as a Living Lab" concept (OSiSoft Data monitoring projects (energy), Cyber data (Scans, Attacks, Advanced Persistent Threats, et al). What has happened at Lehigh to enable this?
- **Mike Shepherd**, I view you as one of or the main points of contact with Internet2 and higher education. Can you elaborate on some of the opportunities Cisco sees coming from the TTP program? How can faculty conducting research that is of potential interest to Cisco navigate with you?

Panel Questions

- Cybersecurity stakes continue to ratchet up. Recall that the CISOs and CIOs at both EquiFax and at Target were immediate casualties of their very public compromises followed shortly by the CEOs. How do we defend use of promising, but unproven information security technologies in the name of supporting research? What if a particular promising solution doesn't pan out?

- Higher education is steadily moving forward with closer collaboration with the private sector in both research, and workforce development. We have representatives of industry and higher education on this panel. What is the ideal relationship for you, and let's start with our industry panelist Mike.

Sample MOU

- UW Madison Cybersecurity Operations Center, Memorandum of Understanding for Faculty Research
- The University of Wisconsin Madison CIO Office ***encourages collaboration between technology researchers and operations staff***. UW-Madison has one of the most complex learning and research laboratories in the form of its campus network and WAN. We ***encourage researchers to share their research*** with us in the hope that we can ***help them to test out, deploy, and fine tune their intellectual property***. We view this as a win-win scenario.
- In order to ensure the highest level of communication between parties who do have different needs and experiences, it ***is important to write down some of the basic understandings that each party has***. We refer to this as a Memorandum of Understanding. We are in the ***process of developing a boilerplate MOU*** to address some of the most important aspects, and are sharing this with other institutions to create a document which can be of value to other institutions as well.

Sample MOU

1. As part of the Office of Cybersecurity, the Cybersecurity Operations Center (CSOC) has been established to protect the University from cyber-attacks of all forms. As such, it is first and foremost an operations center with a primary mission to protect the university.
2. University ***researchers need environments in which to experiment and innovate***. To the extent that their research can be conducted on the university network ***without compromising operations***, it will be considered.
3. The ***workload and mission needs of the CSOC will take priority*** over the timeline and project needs of the researcher. However, every effort will be made to ***balance expectations so that both needs can be addressed***. We understand that faculty research normally has a timeline, and at times intermediate deadlines, that can create a sense of urgency. ***Discussing key deadlines and expectations up front will minimize disappointment and cross communication***.
4. For research projects that require ***risk assessment and certifications*** (e.g., systems under Federal research programs), ***early contact with the Office of Cybersecurity is required*** to ensure required documentation and testing is complete prior to the project beginning work.
5. If an ***NDA*** is required, this will be ***discussed up front before any research begins***.
6. Staff and student staff will function effectively as extended members of the researcher's team. For that reason, it will be ***important for the researcher and the CISO to build a sense of community*** together. ***This is a partnership***.
7. Within calendar year 2018 the CSOC and Office of Cybersecurity will begin to host a vendor provided service which may be used by researchers in the field of firewalls, intrusion detection and intrusion prevention for research projects.

Cybersecurity Research Panel: Network Security

CINC UP: CYBERSECURITY RESEARCH ACCELERATION WORKSHOP & SHOWCASE

AGENDA

- **Cybersecurity Research Panel: Network Security**
  - Alberto Dainotti, University of California-San Diego
  - Dijiang Huang, Arizona State University
  - Johanna Amann, University of California-Berkeley
  - Clifford Neuman, University of California-Berkeley
  - Christos Papadopoulos, Colorado State University
  - Jun Li, University of Oregon
  - Jelena Mirkovic, University of Southern California
- **Cybersecurity Research Panel: Internet of Things**
  - Blaine Reeder, University of Colorado at Denver
- **Cybersecurity Research Panel: Identity & Access Management**
  - Kent Seamons, Brigham & Young University
  - Stanislaw Jarecki, University of California-Irvine
- **Cybersecurity Research Panel: Multidisciplinary Cybersecurity**
  - Shamik Sengupta, University of Nevada

Cybersecurity Research Panel: Network Security

Detecting and Characterizing Internet Traffic Interception Based on BGP Hijacking

Alberto Dainotti
University of California-San Diego

Detecting Internet Traffic Interception based on Route Hijacking

Alberto Dainotti
alberto@caida.org
Center for Applied Internet Data Analysis
University of California, San Diego

Joint work with:
Pavlos Sermpezis, Vasileios Kotronis,
Petros Gigis, Xenofontas Dimitropoulos,
Jae Hyun Park, Danilo Cicalese, Alistair King

Cybersecurity Research Acceleration Workshop and Showcase

October 18, 2017 | San Francisco, CA

ARTEMIS: Neutralizing **BGP Hijacking** within a Minute

Challenge:

Timely detect and neutralize BGP hijacking attacks *(including sophisticated attacks)*

Solution:

- Live BGP monitoring based on public infrastructure and CAIDA's *BGPStream*
- Leverage local knowledge of the network to protect
- Accurate detection rules and heuristics
- Approaches to rapidly mitigate attacks

NSF CNS-1423659
Detecting and Characterizing Internet Traffic Interception based on BGP Hijacking

PI: Alberto Dainotti, *CAIDA, UC San Diego*
alberto@caida.org

Team:

- Pavlos Sermpezis, Vasileios Kotronis, Petros Gigis, Xenofontas Dimitropoulos — *FORTH / University of Crete*
- Danilo Cicalese — *Télécom ParisTech & University Pierre and Marie Curie*
- Alistair King, Jae Hyun Park — *CAIDA, UC San Diego*

Value proposition:

- Protect your network from hijacking and *man-in-the-middle* attacks
- No outsourcing for detection! Autonomously detect events, without sharing private info
- Flexible configuration adapts to your network needs

What we need to TTP

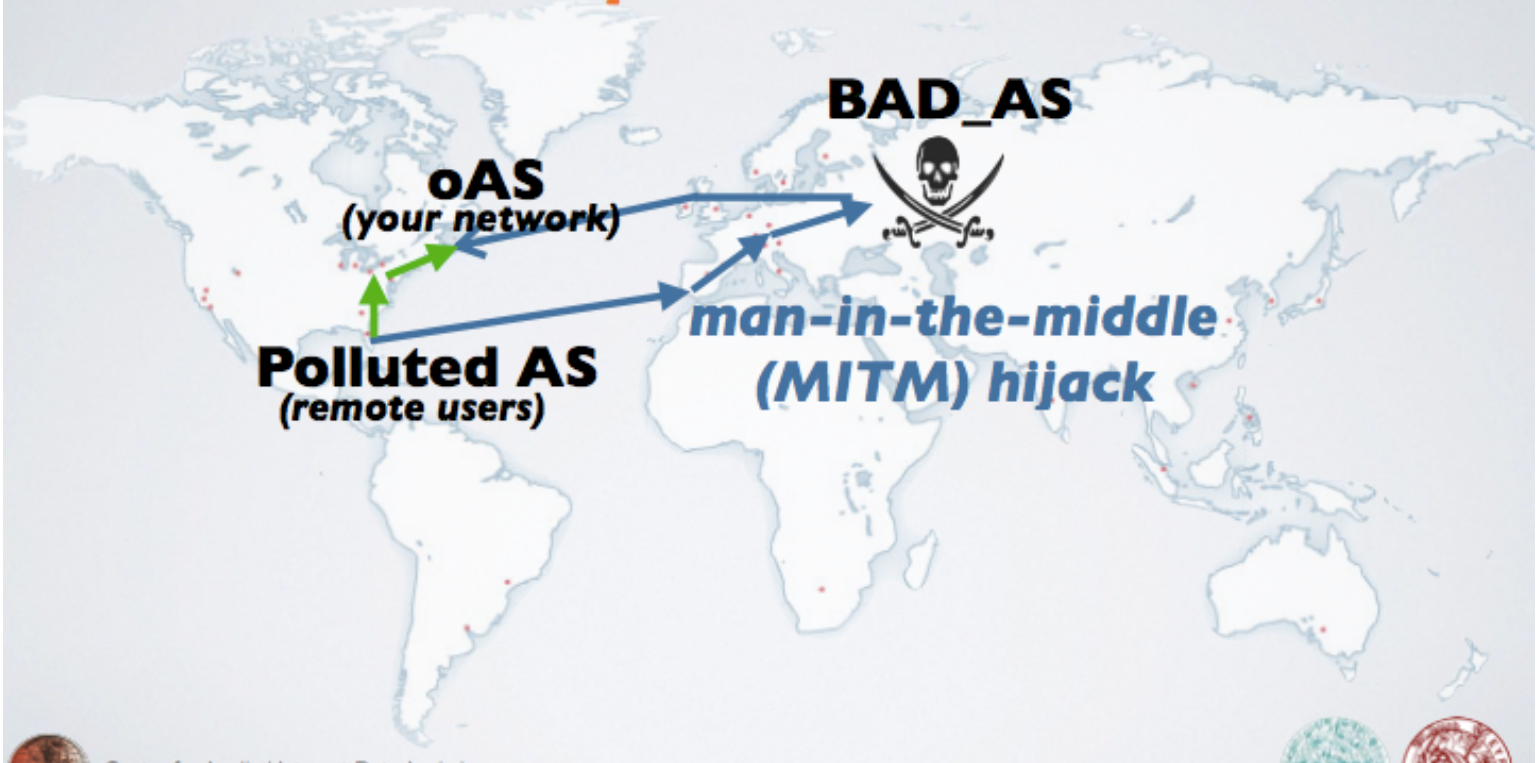
- Setup *ARTEMIS* in your network (assisted pilot program)

INTERNET ROUTE HIJACKING

a threat to your organization and to critical infrastructure

INTERNET ROUTE HIJACKING

a threat to your organization and to critical infrastructure



INTERNET ROUTE HIJACKING

many **MITM** *events documented*

Nov. 2013

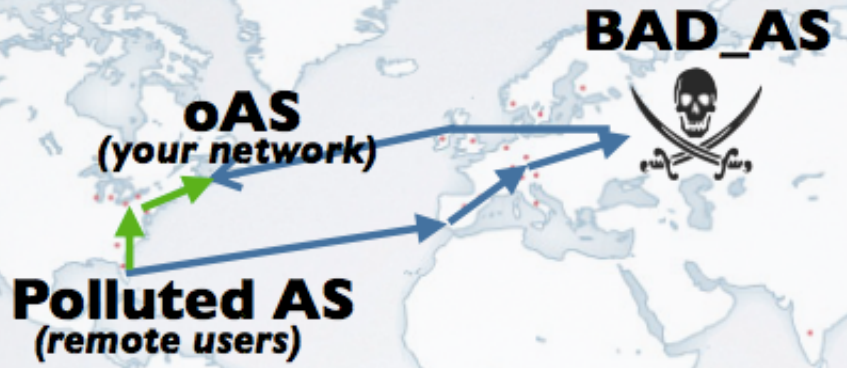
WIRED

The attackers initiated the hijacks at least 38 times, grabbing traffic from about 1,500 individual IP blocks sometimes for minutes, other times for days — and th

http://research.dyn.com/2013/11/mitm-internet-hijacking/

INTERNET ROUTE HIJACKING

many MITM events documented



In few minutes, a single attack can manipulate millions of flows

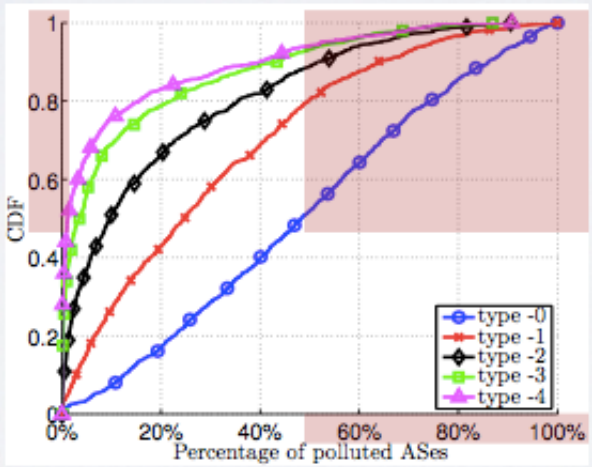
causing: service disruption, fraud, data theft, bad reputation, ...

ATTACKS UNDER THE RADAR

can have large impact

- Hijack Types:
  - **Type 0** hijack: <*prefix:* ***BAD_AS***, …> *(a.k.a. "prefix origin hijack")*
  - **Type 1** hijack: <*prefix: oAS,* ***BAD_AS***, …>
  - **Type 2** hijack: <*prefix: oAS, AS1,* ***BAD_AS***, …>
  - …

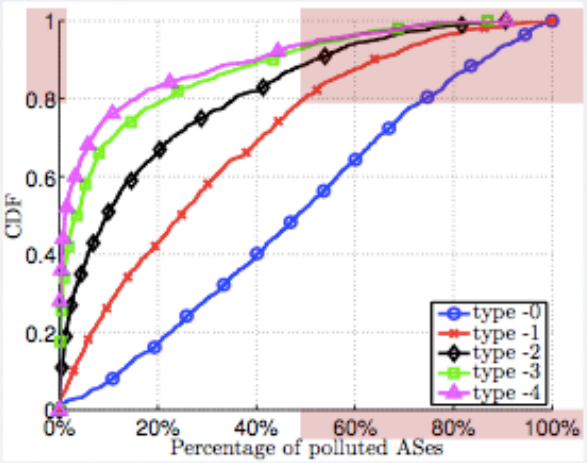
lots of attention



ATTACKS UNDER THE RADAR

can have large impact

- Hijack Types:
  - **Type 0** hijack: <*prefix:* ***BAD_AS***, …> *(a.k.a. "prefix origin hijack")*
  - **Type 1** hijack: <*prefix: oAS,* ***BAD_AS***, …>
  - **Type 2** hijack: <*prefix: oAS, AS1,* ***BAD_AS***, …>
  - …



often neglected

STATE OF THE ART

False Positives + False Negatives

- **Third-party Detection Services**
  - False Positives
    - unless you promptly communicate changes to your network configuration
    - Privacy?
  - False Negatives
    - Most services focus on *Type-0* attacks
    - Hard to detect more sophisticated attacks *(Type-1, Type-2, …)*
  - Mitigation?
    - No integration with mitigation solutions
    - *Btw, would you mitigate if uncertain? how later?*

NEED

EARLY & ACCURATE DETECTION

+

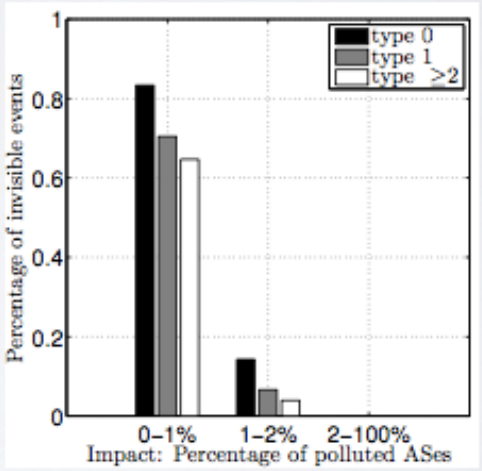
FAST MITIGATION

OUR APPROACH

ARTEMIS (1/3)

- **Realtime BGP Monitoring** using public infrastructure
  - ~200 vantage points worldwide (BGP routers)
    - source: *RouteViews, RIPE RIS, Colorado State Univ. BGPMon*
    - processing: CAIDA's *BGPStream*
  - **Provides visibility of all impactful events**
  - **Detect events in few seconds!**

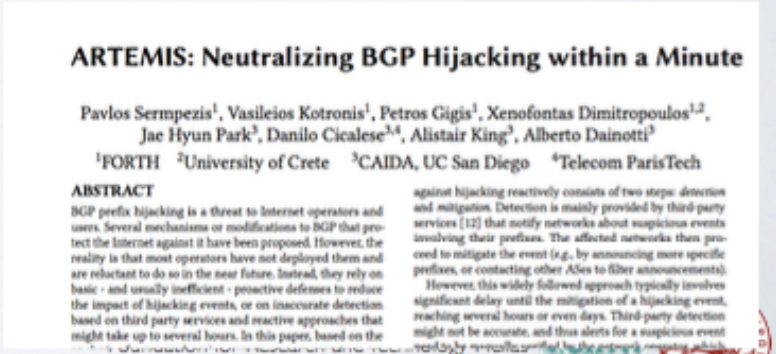
(tested with experiments on the real Internet)



OUR APPROACH

ARTEMIS (2/3)

- **Detection without outsourcing**
  - Run locally: leverages knowledge of your network configuration
  - Accurate:
    - Detects *all* types of attacks!
    - No *false negatives* for all visible attacks
    - No *false positives* for most types of attacks;
      - demonstrated extremely low rate otherwise
  - No sharing of private data
  - Transparency: open source code



ARTEMIS: Neutralizing BGP Hijacking within a Minute

Pavlos Sermpezis[1], Vasileios Kotronis[1], Petros Gigis[1], Xenofontas Dimitropoulos[1,2], Jae Hyun Park[3], Danilo Cicalese[3,4], Alistair King[3], Alberto Dainotti[3]

[1]FORTH [2]University of Crete [3]CAIDA, UC San Diego [4]Telecom ParisTech

ABSTRACT

BGP prefix hijacking is a threat to Internet operators and users. Several mechanisms or modifications to BGP that protect the Internet against it have been proposed. However, the reality is that most operators have not deployed them and are reluctant to do so in the near future. Instead, they rely on basic - and usually inefficient - proactive defenses to reduce the impact of hijacking events, or on inaccurate detection based on third party services and reactive approaches that might take up to several hours. In this paper, based on the

against hijacking reactively consists of two steps: *detection* and *mitigation*. Detection is mainly provided by third-party services [12] that notify networks about suspicious events involving their prefixes. The affected networks then proceed to mitigate the event (e.g., by announcing more specific prefixes, or contacting other ASes to filter announcements).

However, this widely followed approach typically involves significant delay until the mitigation of a hijacking event, reaching several hours or even days. Third-party detection might not be accurate, and thus alerts for a suspicious event

OUR APPROACH

ARTEMIS (3/3)

- **Mitigation**
  - Automated + flexible (it can be configured on a per-prefix basis)
  - Both autonomous or outsourced
    - Prefix de-aggregation
    - Announcement and tunneling from other ASes
    - Contact offending AS and its neighbors

Table 3: Mean percentage of polluted ASes, when outsourcing BGP announcements to organizations providing DDoS protection services.

	without outsourcing	top ISPs	AK	CF	VE	IN	NE
Type0	50.0%	12.4%	2.4%	4.8%	5.0%	7.3%	11.0%
Type1	28.6%	8.2%	0.3%	0.8%	0.9%	2.3%	3.3%
Type2	16.9%	6.2%	0.2%	0.4%	0.4%	1.3%	1.1%
Type3	11.6%	4.5%	0.1%	0.4%	0.3%	1.1%	0.5%

ARTEMIS CONFIGURATION

sample

- **Configuration file**
  - configure manually
  - extract from routers / route reflector
  - pre-populate from RADB?
  - …

```
// Artemis configuration for our main prefixes
prefixes: 123.123.0.0/16, 111.111.111.0/24
  origin_asns: 4131, 4132
  neighbors: 4000, 3112, 2670, 45, 2800, 7462, 4123
  mitigation: deaggregate

// Artemis configuration for prefixes we use only at site #2
prefixes: 123.124.125.0/24, 222.222.222.0/24
  origin_asns: 4131
  neighbors: 2800, 7462, 4123
  mitigation: deaggregate, outsource
```

PILOT DEPLOYMENT

try ARTEMIS

- **Pilot** deployment of detection component
  - *all you need is a box with Python*
- Feedback
- Read our paper draft
- Contribute to the development of scripts etc.

THANKS

alberto@caida.org

Center for Applied Internet Data Analysis
University of California San Diego

Foundation for Research and Technology-Hellas
University of Crete,

ONE LAST SLIDE

*- We are also developing a centralized service (**an Internet observatory for BGP hijacks and anomalies**) which does not need deployment in your network*

- Soon you'll be able to subscribe to receive notifications and inspect events on a dashboard

- If you upload your ARTEMIS configuration file it is going to be more accurate and may provide more information about the incident

SRN: On Establishing Secure and Resilient Networking Services

Dijiang Huang
Arizona State University

cynetllc.com

SRN: On Establishing Secure and Resilient Networking Services

"All War is based on Deception"

- Sun Tzu, Art of War

Sponsored by

Cybersecurity Research Acceleration Workshop and Showcase

October 18, 2017 | San Francisco, CA

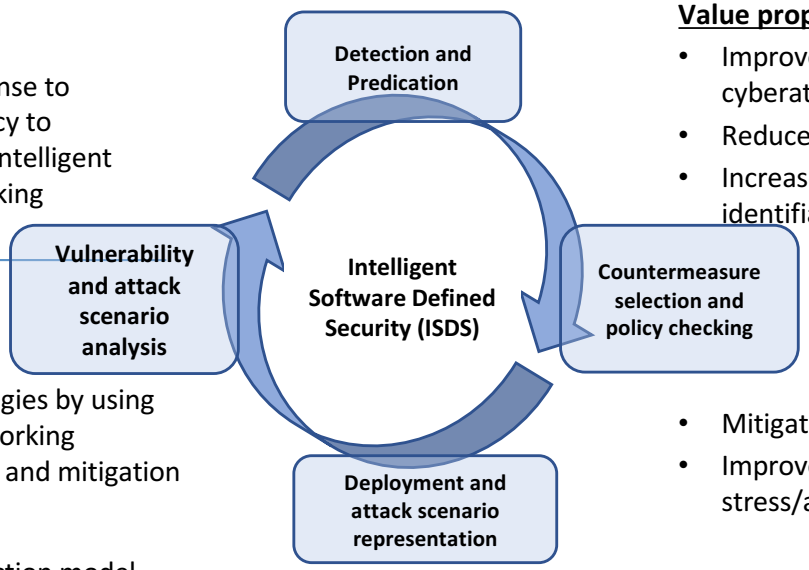
Quad Chart for: SRN: On Establishing Secure and Resilient Networking Services

Challenge:

Using moving target defense to improve network resiliency to cyberattacks through an intelligent software-defined networking approach.

Solution:

- Design intelligent security defense strategies by using software defined networking approaches to prevent and mitigation attacks effectively.
- Devise an attack prediction model based on security situation monitoring and intrusion detection.
- A comprehensive countermeasure selection and deployment model to improve security resiliency and reduce intrusiveness to good users.



NSF NSF SaTC CNS 1528099

PIs: Dijiang Huang (ASU), Kishor Trivedi (Duke), Deep Medhi (UMKC)

Contact us

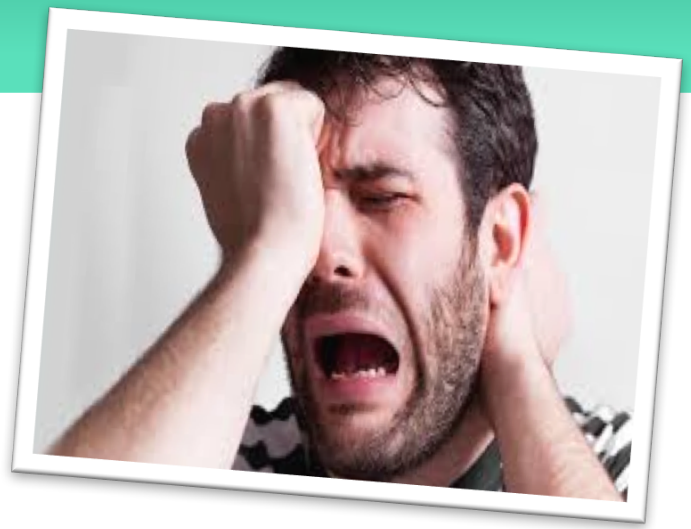
- Dijiang.huang@asu.edu
- ktrivedi@duke.edu
- dmedhi@umkc.edu

Value proposition:

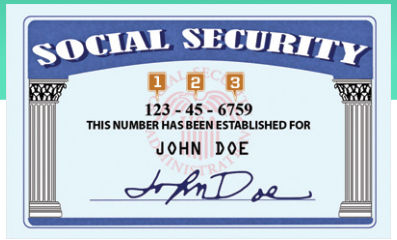
- Improve the agility and resiliency to cyberattacks.
- Reduce human-in-the-loop pitfalls
- Increase attackers' cost (effort and identifiability)
- Mitigate attack consequence/impact
- Improve the service continuity under stress/attacks

What we need to TTP

- Produce Minimum Viable Product (MVP) for pilot projects or trials
- Seek investments or licensing
- Establish a spin-off company

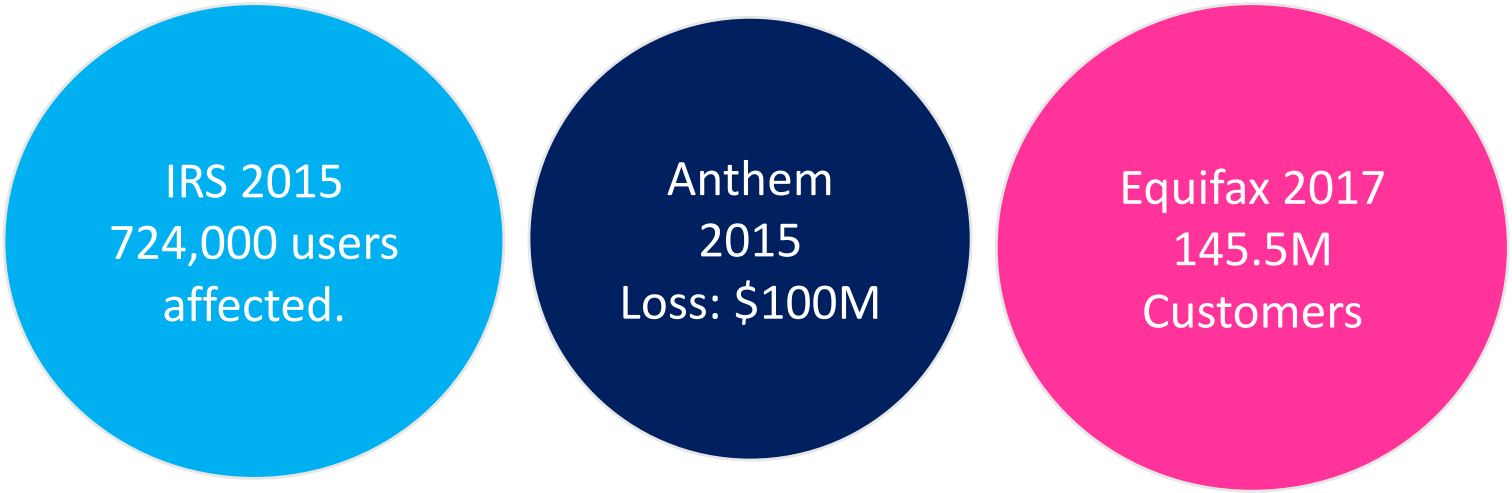


Anthem BlueCross



PayPal

Security is a Reactive Problem



PROBLEM

SINGLE TARGET

Unintelligent Security?

- Not easy to make changes **automatically** and **quickly** to adjust security defense system based on current security situations

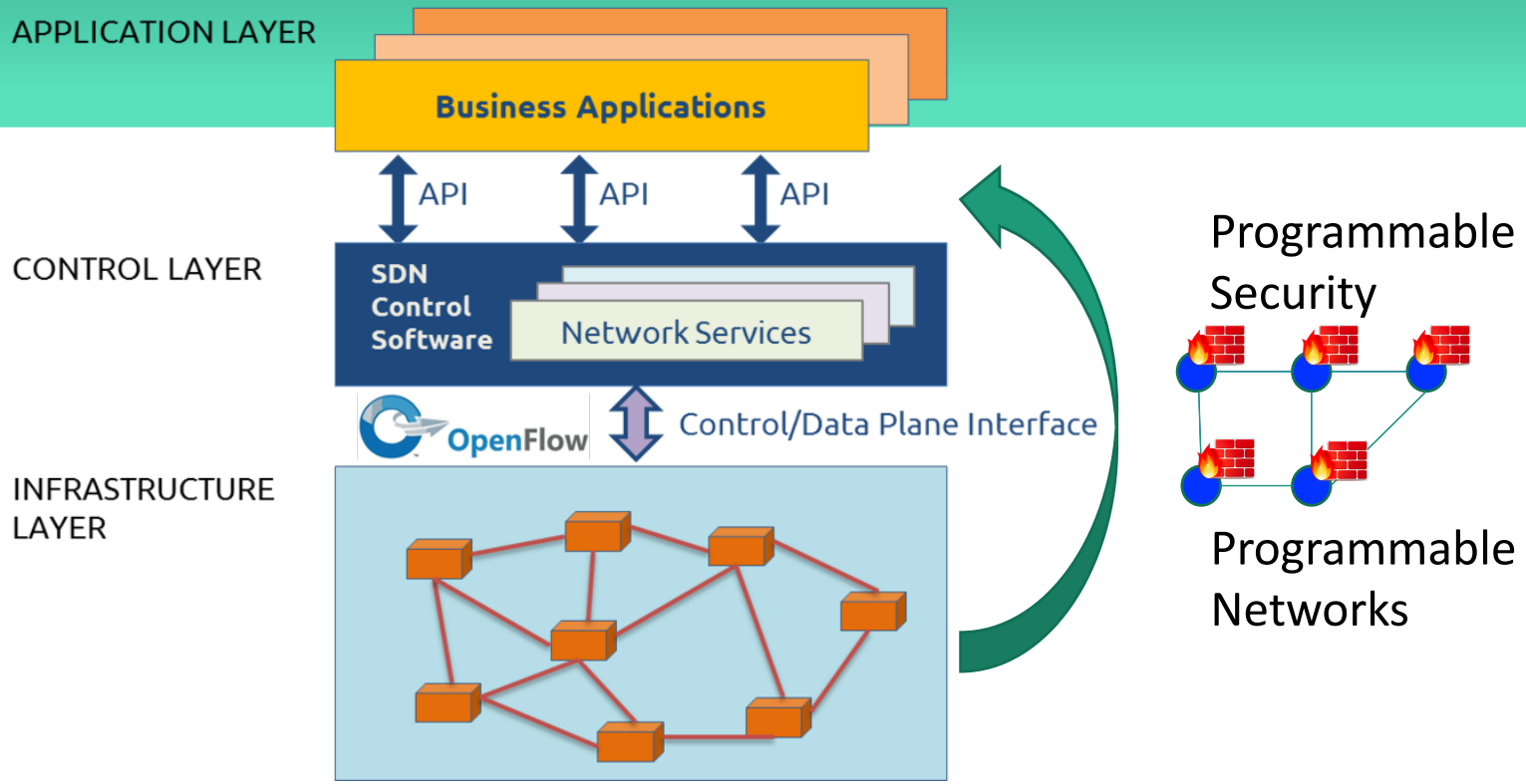
  - little programmability,
  - defense goals are predefined,
  - human-in-the loop,
  - lack of learning, planning, and execution capabilities.

“Art of War is based on Deception”

- Sun Tzu, Art of War

MOVING TARGET DEFENSE

Software Defined Networking and Security



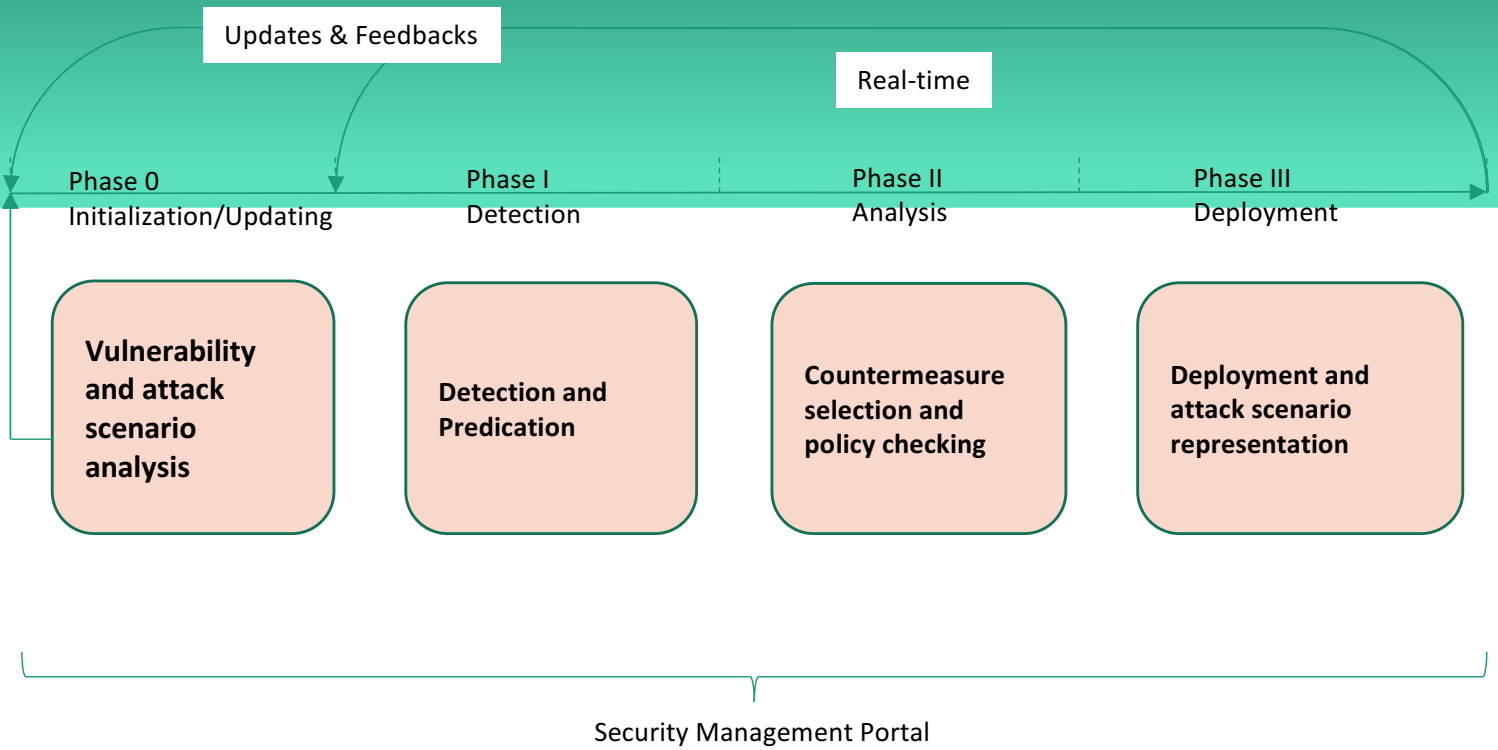
What is intelligent and software-defined security?

- **Reactive → Proactive**
  Act before attackers and reduce the bad consequence.

- **Static → Dynamic:**
  Use virtualization and programmable approaches to automate security defense approaches

- **Intelligently shift and change over time**
  Smartly (re)configure the security system to **increase the complexity to attackers**, **reduce the attack surfaces** with **minimal level of intrusiveness** to good users.

Overview: A Network ISDS Architecture (Four Phases)



COST AND RISK REDUCTION

70% to 4%

man-power reduction for security analysis.

96%

Reduction in security attacks

Based on our testing results from Science DMZ platform

Proven Technology

- Ongoing Pilot project talk with NCI inc. and State Farm.
- ASU Science DMZ Internet2.

JOURNEY..

- Over $1M research, equipment, and development grant from ONR and NSF to develop the intelligent SDN security technology from 2013 to 2018.
- 5 provisional Patents, 1 issue US Patent.
- $667K NSF SaTC (with TTP) award
- $22,500 award at ASU New Venture Challenge.

cynetllc.com

Dijiang Huang

dijianghuang@cynetllc.com

dijiang@asu.edu

Demo Video

Effective and Economical Protection for High-Performance Research and Education Networks

Johanna Amann
University of California-Berkeley

Effective and Economical Protection for High-Performance Research and Education Networks

Johanna Amann

johanna@icir.org

Cybersecurity Research Acceleration Workshop and Showcase

October 18, 2017 | San Francisco, CA

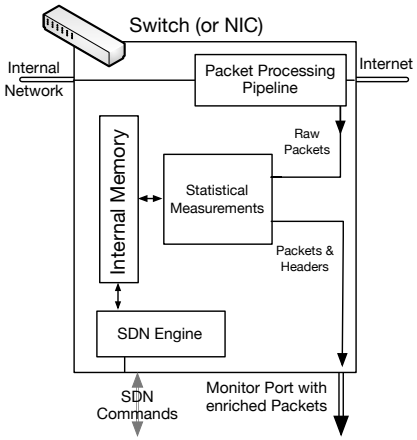
Quad Chart for: Effective and Economical Protection for High-Performance Research and Education Networks

Challenge:

- Increase performance of network monitoring for high-speed scientific environments.
- Expand visibility into research and education networks.

Solution:

- Hardware/Software co-design with:
  - Accelerated statistics
  - Connection establishment offloading
  - TCP stream reassembly
  - Hardware pattern matching
- Advance visibility for R&E networks:
  - Support domain-specific protocols
  - Enable network profiling
  - Enable better active response
  - Enforce security policies



NSF ACI #1642161
ICSI

PI: Johanna Amann (ICSI)
Co-PIs: Robin Sommer (ICSI), Michael Dopheide (Esnet)

Impact:

- Enable better protection of high-speed research and education networks, specifically DMZ environments.
- Integrates with Bro network monitor already widely used in R&E community.

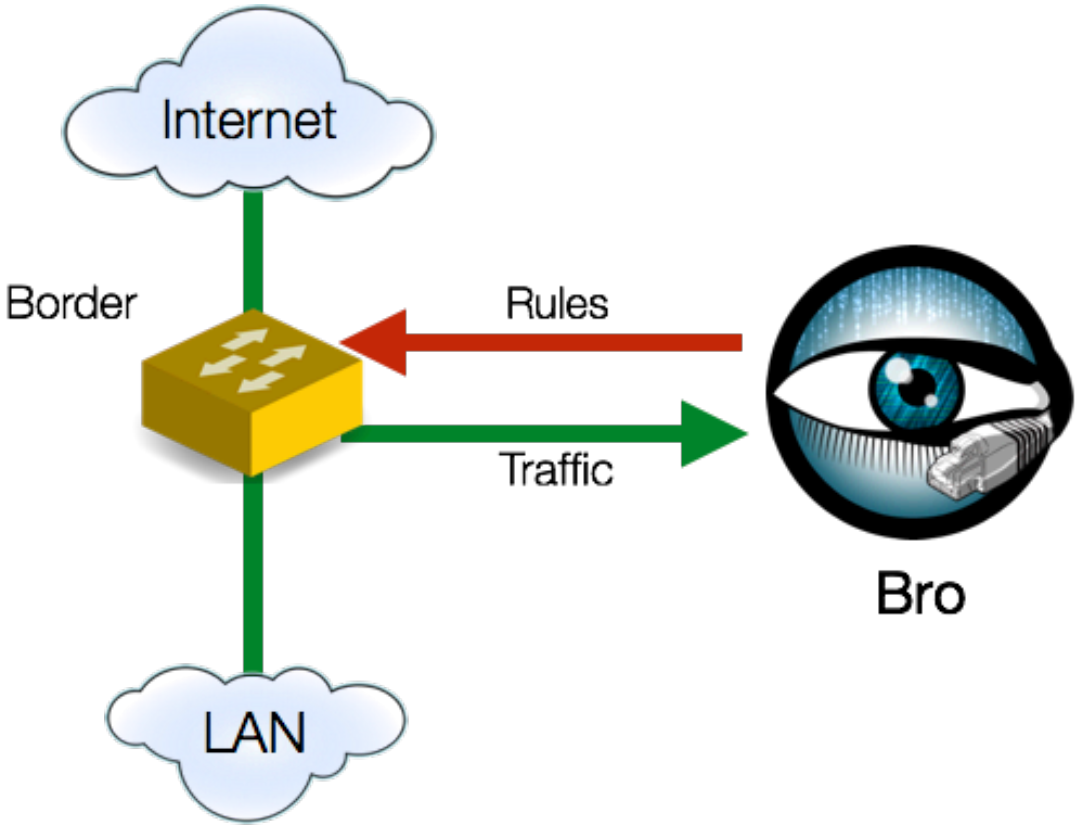
What we need:

- Your feedback on
  - Network visibility issues
  - Protocols used in environments
  - Current monitoring performance pain points

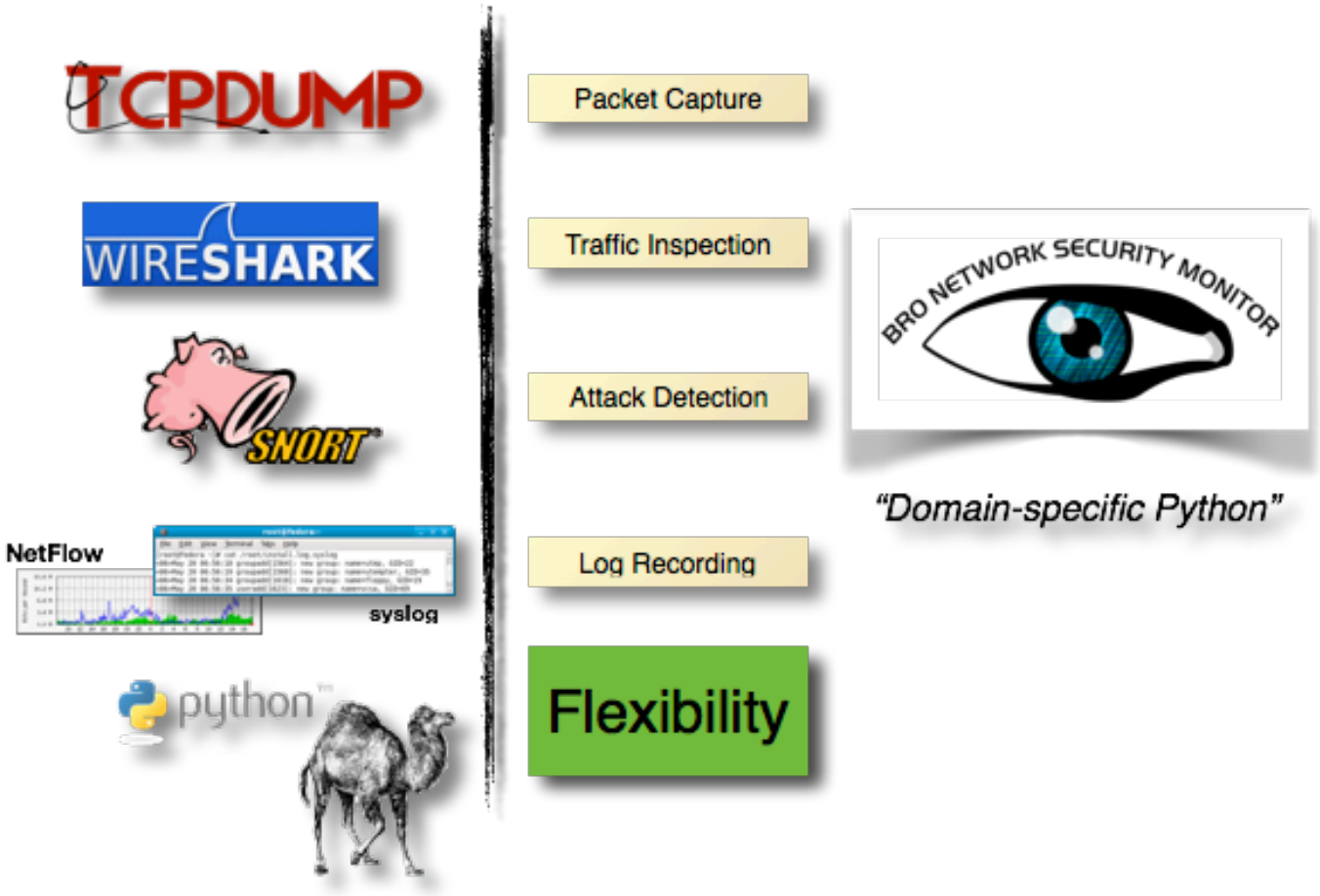
Contact:

- johanna@icir.org
- robin@icir.org
- dopheide@es.net

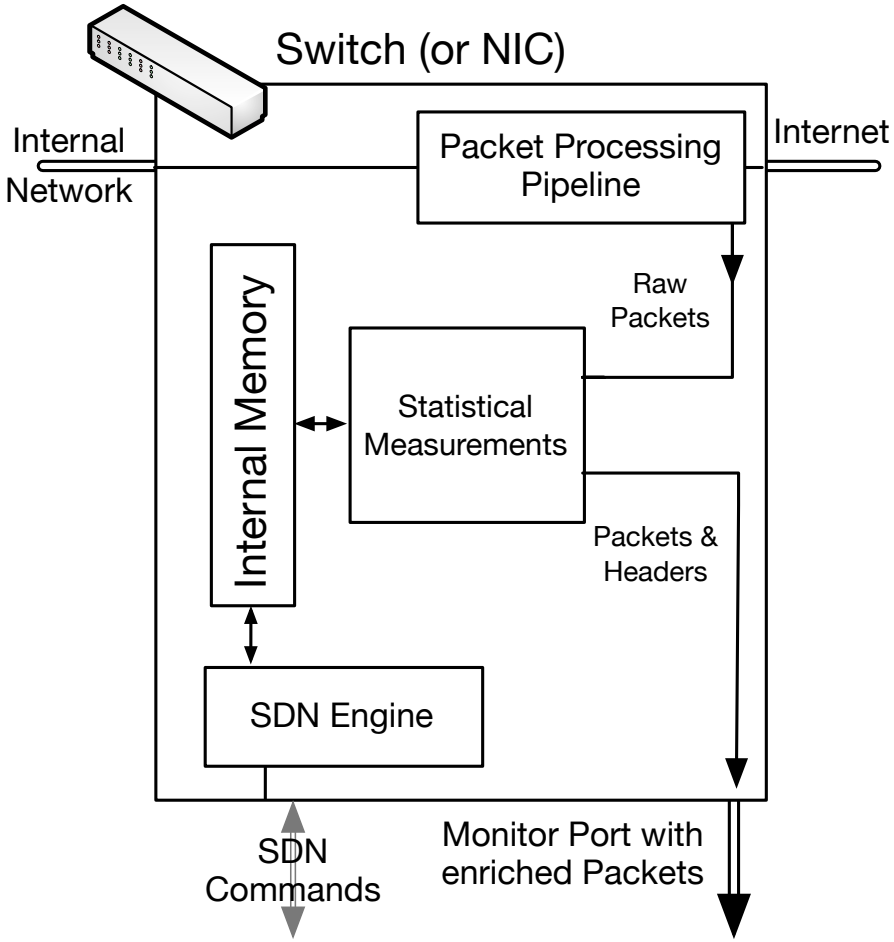
Typical Network Monitoring Setup



What is Bro?


TCPDUMP
WIRESHARK
SNORT
NetFlow
syslog
python
Packet Capture
Traffic Inspection
Attack Detection
Log Recording
Flexibility
BRO NETWORK SECURITY MONITOR
"Domain-specific Python"

Hard/Software Co-Design for Network Monitoring



Domain-Specific Security Monitoring

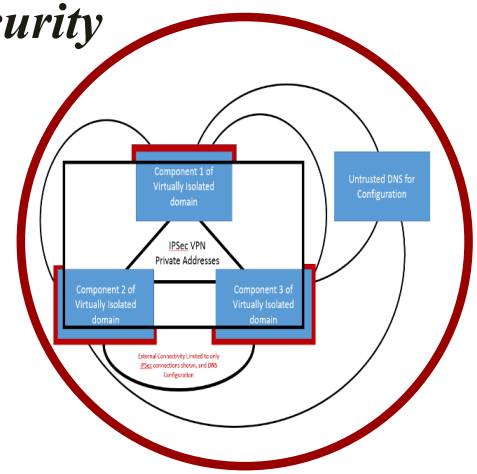
- Domain-specific protocols
- User authentication
- Network activity profiling
- Security policy enforcement
- DOS Protection

Distributed Virtually Isolated Domains

Clifford Neuman
University of Southern California

Distributed Virtually Isolated Domains

Clifford Neuman
Director, Center for Computer Systems Security
Information Sciences Institute
University of Southern California



Cybersecurity Research Acceleration Workshop and Showcase

October 18, 2017 | San Francisco, CA

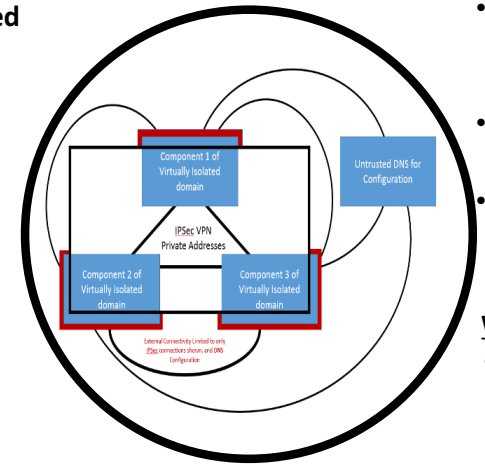
Quad Chart for: Distributed Virtually Isolated Domains

Challenge:

- **Enable rapid deployment of distributed applications with limited attack surface from the Internet.**
- **Provided containment from exfiltration and subversion.**
- **Protect Internet from student experiments**

Solution:

- **Dynamic IPsec deployed VPN over leaf nodes (no permanent nodes)**
- **Configuration/establishment of VPN uses a DNS dynamically for configuration.**
- **Nodes in the domain run special victual machine, for bare metal OS that establishes tunnels for communication and blocks all else.**



Value proposition:

- Inbound isolation for protected applications, dependent upon security of the “hosts”.
- Reduced attack surface for subversion or exfiltration.
- Outbound application isolation based on security of the “guest” or “hypervisor”.

What we need to TTP

- Distributed applications that don’t require exchange of information outside the isolated components.
- Classes looking to provide isolated environment for students utilizing resources on students and instructors own computers.

Contact us

- PI: Prof. Clifford Neuman
  Center for Computer Systems Security
  University of Southern California
  bcn@isi.edu

Today's Systems Less Secure

- Functional requirements for today's distributed applications eliminate isolation.
  - Larger attack surface – applications and server interfaces reachable through the Internet.
  - Users demand instant access to their data from all devices, wherever they may be.
  - Users demand ability to move data between applications.
- But not all "applications" should allow this much sharing.
  - We need to restore isolation, but along functional boundaries.

© Can Stock Photo

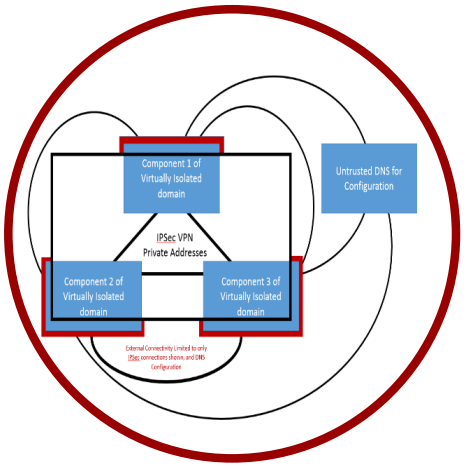
Many existing technologies *support* isolation

- Within computer systems
  - Virtual Memory
  - Virtualization
  - Trusted computing
  - Data Encryption
- Within Computer Networks
  - Firewalls
  - Virtual Private Networks
  - Communication encryption

- But our policies are too complex
  - Because they support isolation **and** sharing.

Changing our Concept of Isolation

- Changing the way we think of isolation
  - Not about artificial physical boundaries that are artifacts of how we build our systems
  - But rather around virtual boundaries that map onto the conceptual functions for which we use the systems.



Transition to Practice

- CentOS Extended to configure VM's or bare-metal systems in isolated domains.
  - FreeS/WAN IPSec tunnels to connected components
  - IP tables, internal configuration, and addressing prevent direct access to external internet)
  - Limits external subversion and internal exfiltration by reducing attack
  - Used for classes and CTF type exercises
  - Has been integrated with the DETER testbed for hybrid experiments.
- Further reduction of attack surface
  - Move network management into hypervisor (smaller code)
  - Consider appliance (e.g. firewall) - creates problem for attestation of systems inside the domain.
- Management of domains
  - Use of directory service to hold certificates for member components and dynamic address information.
  - This allows one to join a domain given its name, and a key or other authentication information.
  - Vulnerable to violations of availability policy, but information flow policies (subversion and exfiltration) not affected by directory service.
- Policy Management
  - Ability for a hardware/software component to join a domain based on domain's policy and accreditation of components.
- Performance
  - Use of trusted computing and accredited OS's to manage ability to join a domain.
- Contact us – bcn@isi.edu

Survey Tools to Collect Feedback

Workshop Overall:
http://bit.ly/ttptechexws

Researcher Assets:
http://bit.ly/ttptechexresearch

Cybersecurity Research Panel: Network Security

NETBRANE: A Software Defined DDoS Protection Platform

Christos Papadopoulos
Colorado State University

Homeland Security
Science and Technology

2017 | Cyber Security Division
DDoSD Program

Netbrane: A Software-Defined DDoS Protection Platform for Internet Services

Colorado State University
Christos Papadopoulos

Cybersecurity Research Acceleration Workshop - Oct 18, 2017 – San Francisco CA

Colorado State University

Cybersecurity Research Acceleration Workshop and Showcase

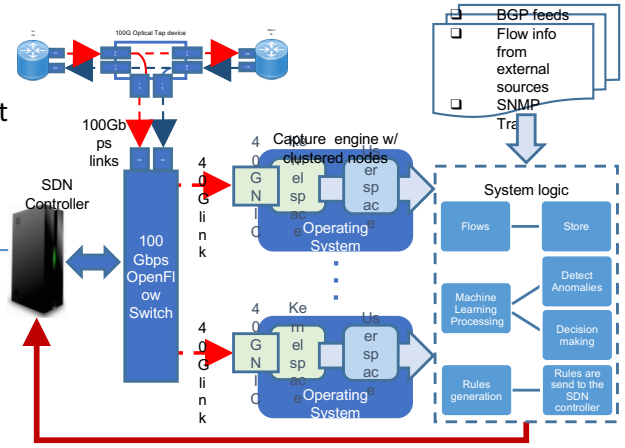
October 18, 2017 | San Francisco, CA

UCR

Quad Chart for: Cybersecurity Transition To Practice (TTP) Acceleration NetBrane: A Software-Defined DDoS Protection Platform for Internet Services

Challenge:

Build an effective, pro-active defense system for DDoS attacks at an Internet scale



Solution:

- High-speed capture (100Gbps and more)
- Traffic modeling using Machine Learning for low false positives and negatives, near real-time model fitting and classification
- Combination of network maps, BGP routing , vulnerable servers, etc, to proactively develop responses
- SDN technology for attack mitigation
- Hacker chatter capture, NLP processing, actionable alerts

What we need to TTP

- Access to operational traffic to develop accurate models
- Opportunities to deploy our prototype at IXPs

DHS D15PC00205
Colorado State University

PI: Christos Papadopoulos
Team: Stephen Hayne, Haonan Wang, Michalis Faloutsos

Value proposition:

- Unprecedented insight into traffic at a network via collection of very fine granularity information
- Distributed alert system to propagate strategic information to all networks
- Proactive defenses that minimize collateral damage
- Powerful SDN filters that support thousands of rules
- Hacker chatter alerts to plan defenses ahead of an attack

Contact us

- christos@colostate.edu
- Stephen.Hayne@colostate.EDU
- haonan.wang@gmail.com
- michalis@cs.ucr.edu

Team Profile

The Team:

- Colorado State University:
  - **Stephen Hayne**, Dimitris Kounalakis, Robert McAndrew, **Christos Papadopoulos**, Ela Sienkiewics, Spiros Thanasoulas, **Haonan Wang**
- University of California, Riverside:
  - Ahmad Darki, **Michalis Faloutsos**, Joobin Gharibshah, Mike Li

Colorado State University

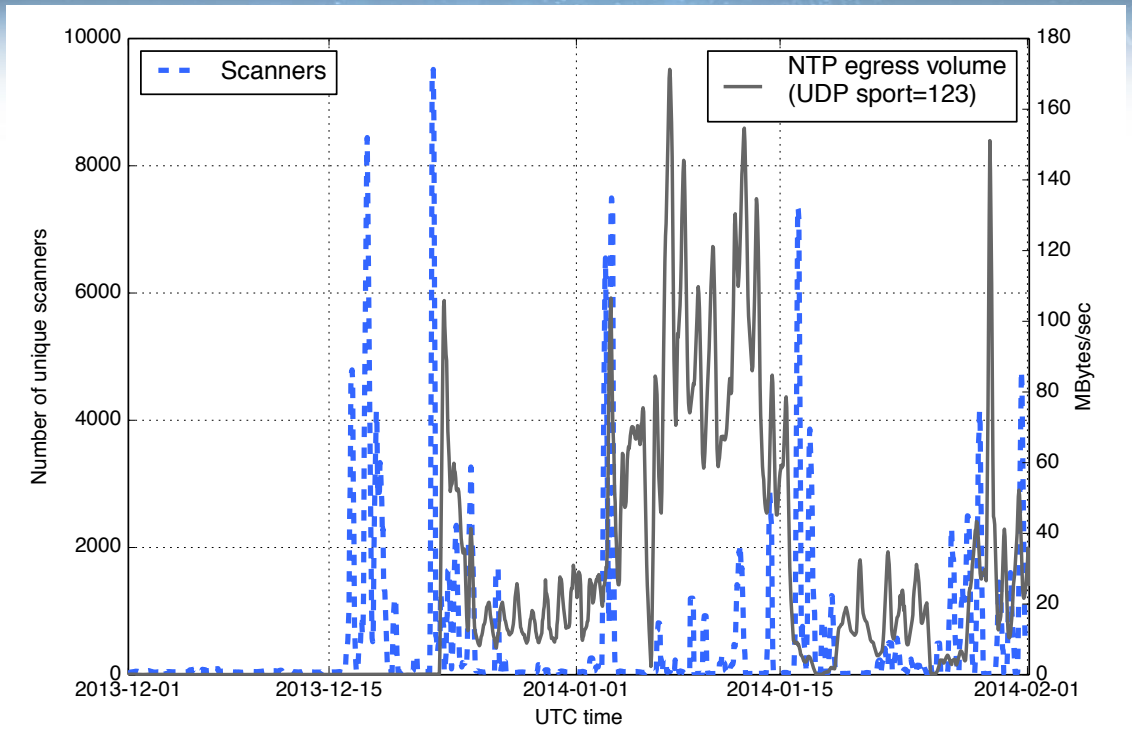
Value Proposition

- Distributed Denial of Service (DDoS) attacks will be at the top of security threats for the foreseeable future

- State of the Art DDoS defense today:
  - Intentionally hijack traffic, redirect to scrubbing centers, tunnel back to customer
  - Expensive, small clean pipe, susceptible to collateral damage

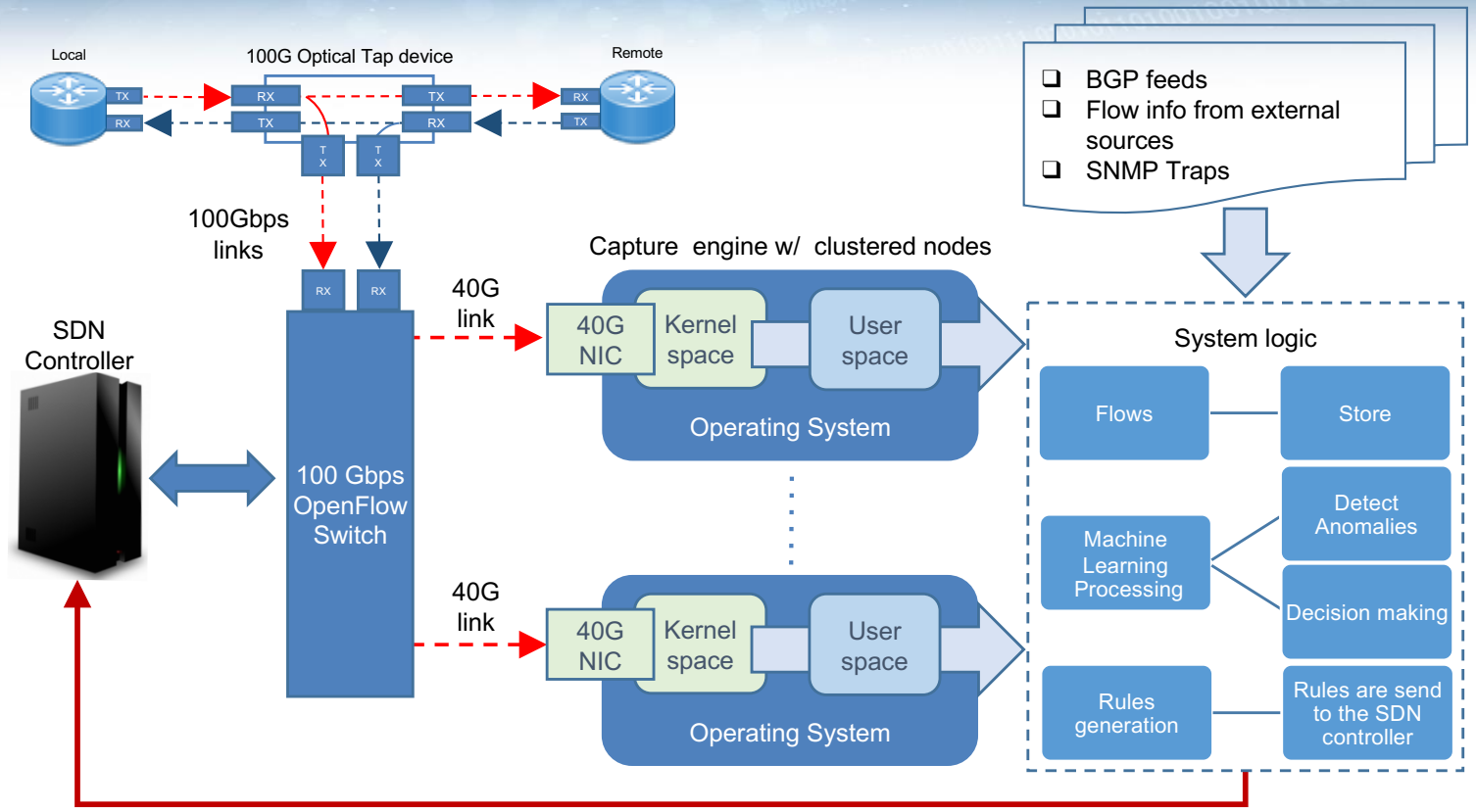
- Need to be distributed, effective and proactive:
  - Reliably detect the attack using machine learning, create filtering rules
  - Communicate filters to your upstreams immediately
  - High-capacity SDN switches to block attack
  - Defense readiness via network structural information and hints from hacker forums

Can Attacks Be Predicted?

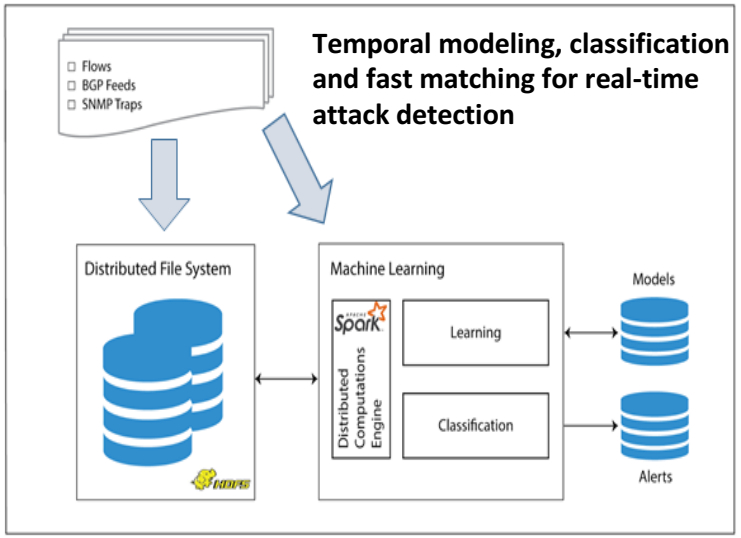


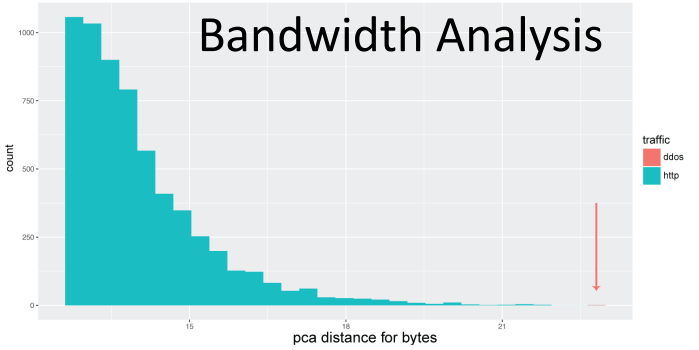
Scanning activity before 2014 NTP attacks offered clues

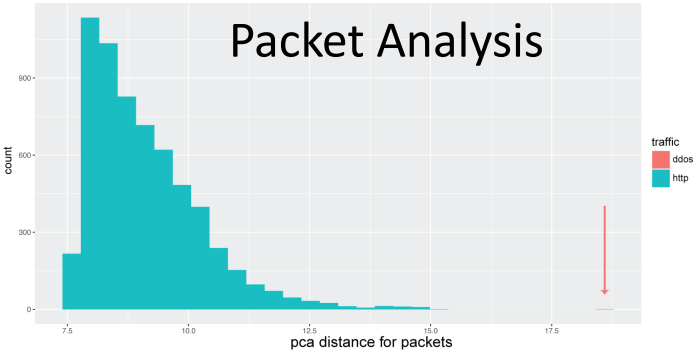
System Architecture



Machine Learning Component





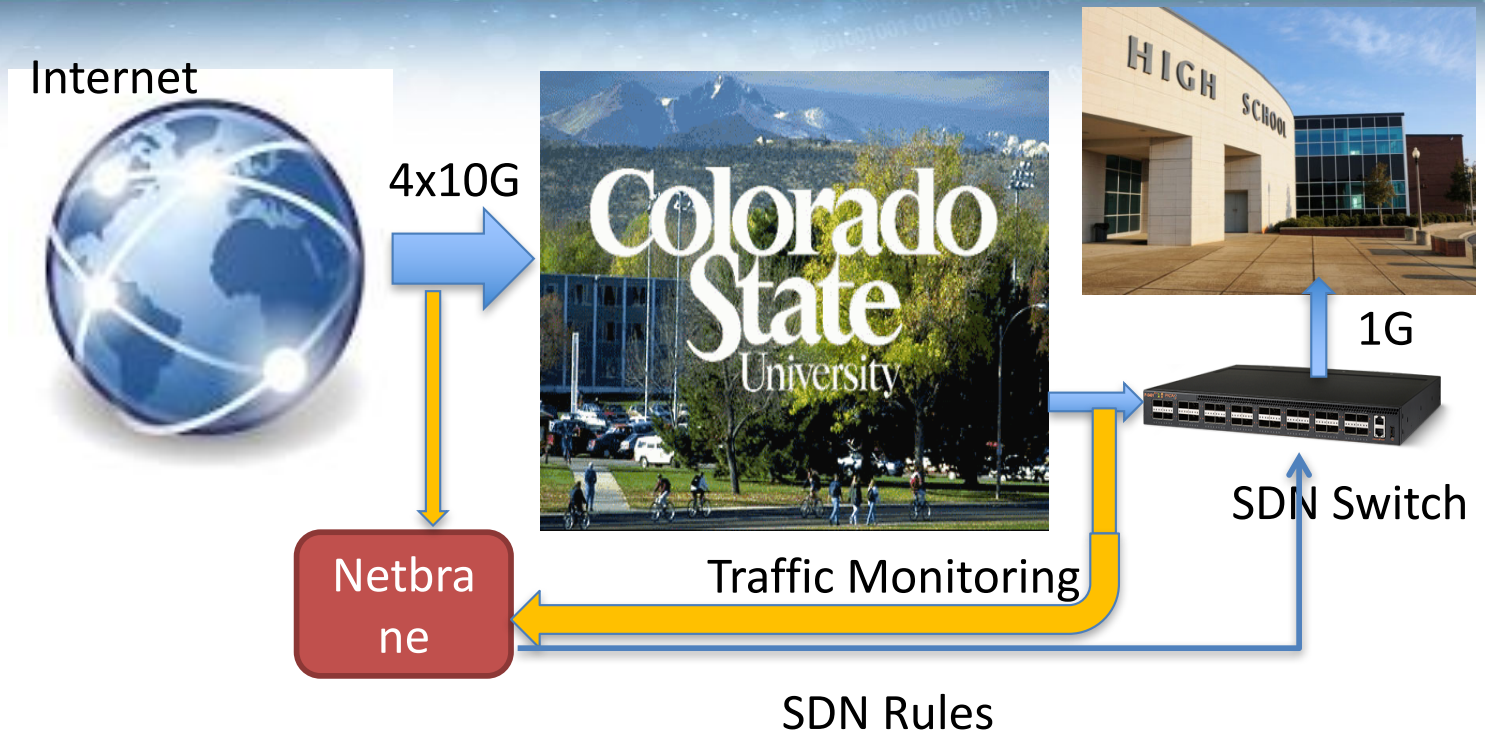


With Machine Learning attacks that were not Visible before, easily stand out

Deployment

- Pilot at CSU (ongoing)
- Larger deployment at our regional ISP (FRGP) within a year
- Expanded deployment with other upstreams immediately after that
- Requirements:
  - Optical taps for attack detection
  - 2-4U for local compute (packet->flow conversion)
  - Access to a cloud provider for ML processing
  - SDN switch for mitigation

Current Prototype Deployment



Deploying Netbrane prototype to protect a CSU customer (in progress)
Netbrane on our regional ISP (planned)

Contact Information

Christos Papadopoulos
Colorado State University
christos@colostate.edu
+1-970-491-3267

Stephen Hayne
Colorado State University
Stephen.Hayne@ColoState.EDU
+1-970-491-7511

Michalis Faloutsos
University of California Riverside
michalis@cs.ucr.edu
+1-951-907-1501

DrawBridge 2.0 – Bringing Software-Defined DDoS Defense To Fruition

Jun Li
University of Oregon

Cybersecurity Research Acceleration Workshop and Showcase

October 18, 2017 | San Francisco, CA

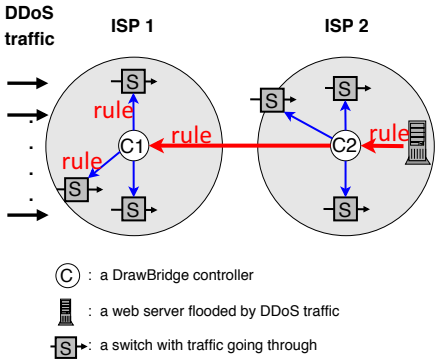
Quad Chart for: (DrawBridge 2.0—Bringing Software-Defined DDoS Defense To Practice)

Challenge:

Need many Internet service providers to adopt DrawBridge and build a collaborative defense of distributed denial-of-service (DDoS).

Solution:

- Collect real-world input from potential DrawBridge adopters and subscribers
- Enhance DrawBridge code with more modules toward real settings
- Stress test DrawBridge on a designated subnet and GENI
- Test and improve user experience with UONet
- Experiment with DrawBridge and two ISPs—UONet and NERO
- Experiment with DrawBridge and multiple ISPs—UONet, NERO, Internet2, and others



This project is in part the result of funding provided by the Science and Technology Directorate of the United States Department of Homeland Security under contract number D15PC00204. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security or the US Government.

Value proposition:

- DrawBridge empowers DDoS victims to dictate what traffic can or cannot be delivered to them
- With a minimum number of highly effective rules generated on the fly by observing incoming DDoS traffic,
- And then placed at selected locations inside the DrawBridge network

What we need to TTP

- DrawBridge adopters to run DrawBridge service
- DrawBridge subscribers to sign up to be protected from DDoS
- Develop and execute a business plan
- Your feedback and comments

Contact us

- Email: lijun@uoregon.edu
- Phone: 541-852-5580
- Skype: softlaser2

This project is in part the result of funding provided by the Science and Technology Directorate of the United States Department of Homeland Security under contract number D15PC00204. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security or the US Government.

DrawBridge 2.0:

Bringing Software-Defined DDoS Defense To Practice

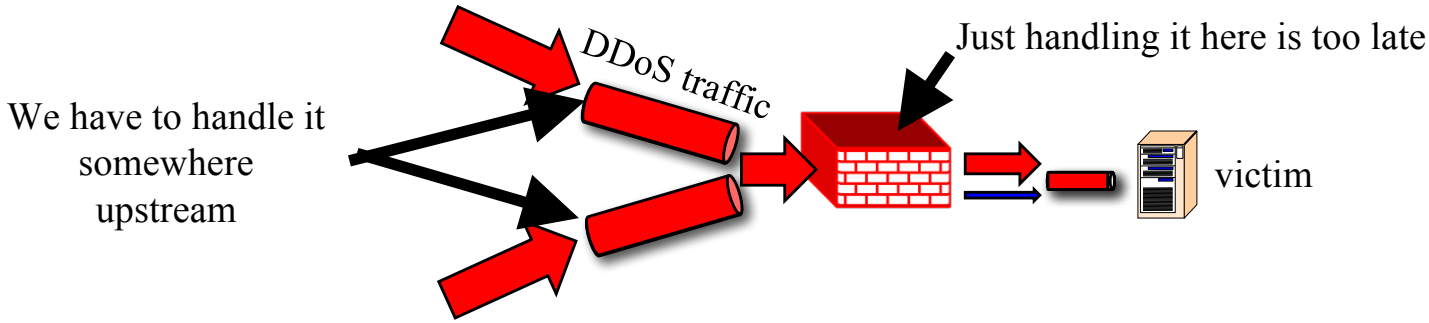
Jun Li
Professor, Computer and Information Science
Director, Center for Cyber Security and Privacy
University of Oregon

Contact info:

- Email: lijun@uoregon.edu
- Phone: 541-852-5580
- Skype: softlaser2

Customer Need

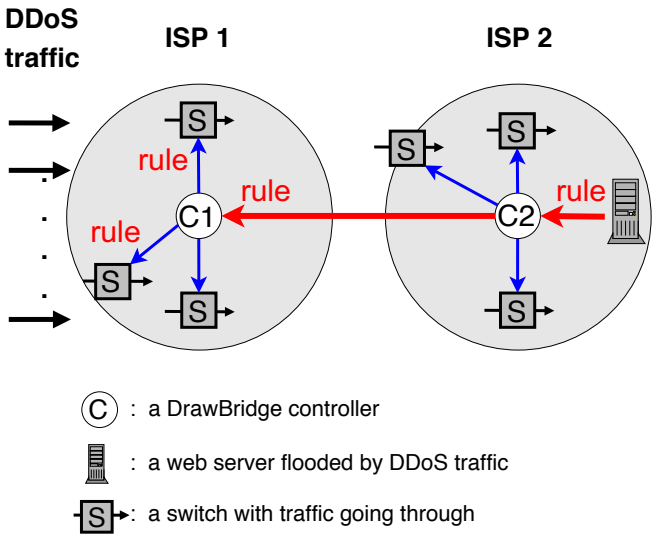
- DDoS attacks continue to be devastating
- Victims are best able to determine which traffic should be delivered to them
- But least able to control that decision
- ISPs, on the other hand, are able to drop the DDoS packets but do not really know which traffic to drop



UNIVERSITY OF OREGON

The DrawBridge Approach

- Our solution, DrawBridge, will enable its users to inform ISPs how to handle DDoS attacks
  - On attack, the user generates and sends DDoS-filtering rules to the DrawBridge controller at an upstream ISP
  - The controller verifies and deploys the rules at well-chosen switches or upstream ISPs to filter DDoS traffic
  - All communication uses the DrawBridge protocol to ensure efficiency and security
- DrawBridge is based on **software-defined networking** (SDN), which is well-suited for traffic handling tasks—including filtering traffic that meets specific rules or criteria



UNIVERSITY OF OREGON

Bringing DrawBridge To Practice

- We have developed a prototype of DrawBridge as well as demos of how DrawBridge works
- To further bring DrawBridge to practice, we will:
  - Collect real-world input from potential DrawBridge adopters and subscribers
  - Enhance DrawBridge code with more modules toward real settings
  - Stress test DrawBridge on a designated subnet and GENI
  - Test and improve user experience with UONet
  - Experiment with DrawBridge and two ISPs—UONet and NERO
  - Experiment with DrawBridge and multiple ISPs—UONet, NERO, Internet2, and others
- We will particularly need the following help:
- DrawBridge adopters to run DrawBridge service
- DrawBridge subscribers to sign up to be protected from DDoS
- Develop and execute a business plan
- Your feedback and comments

UNIVERSITY OF OREGON

Quad Chart for:

Cybersecurity Research Acceleration Workshop and Showcase

October 18, 2017 | San Francisco, CA

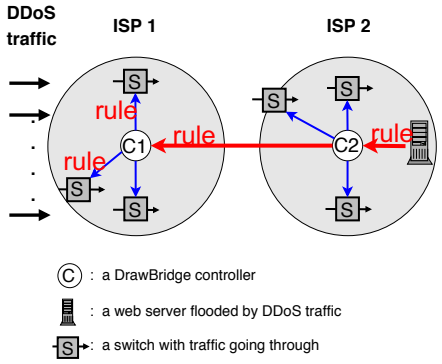
Cybersecurity Transition To Practice (TTP) Acceleration (DrawBridge 2.0—Bringing Software-Defined DDoS Defense To Practice)

Challenge:

Need many Internet service providers to adopt DrawBridge and build a collaborative defense of distributed denial-of-service (DDoS).

Solution:

- Collect real-world input from potential DrawBridge adopters and subscribers
- Enhance DrawBridge code with more modules toward real settings
- Stress test DrawBridge on a designated subnet and GENI
- Test and improve user experience with UONet
- Experiment with DrawBridge and two ISPs—UONet and NERO
- Experiment with DrawBridge and multiple ISPs—UONet, NERO, Internet2, and others



Value proposition:

- DrawBridge empowers DDoS victims to dictate what traffic can or cannot be delivered to them
- With a minimum number of highly effective rules generated on the fly by observing incoming DDoS traffic,
- And then placed at selected locations inside the DrawBridge network

What we need to TTP

- DrawBridge adopters to run DrawBridge service
- DrawBridge subscribers to sign up to be protected from DDoS
- Develop and execute a business plan
- Your feedback and comments

Contact us

- Email: lijun@uoregon.edu
- Phone: 541-852-5580
- Skype: softlaser2

UNIVERSITY OF OREGON

SENSS - Security Service for the Internet

Jelena Mirkovic
University of Southern California

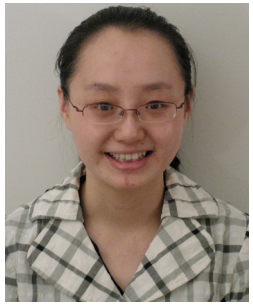
USC University of Southern California

facebook

Yale University

SENSS

Security Service for the Internet

Jelena Mirkovic (USC/ISI), Minlan Yu (USC), Ying Zhang (HP Labs), Sivaram Ramanathan (USC)

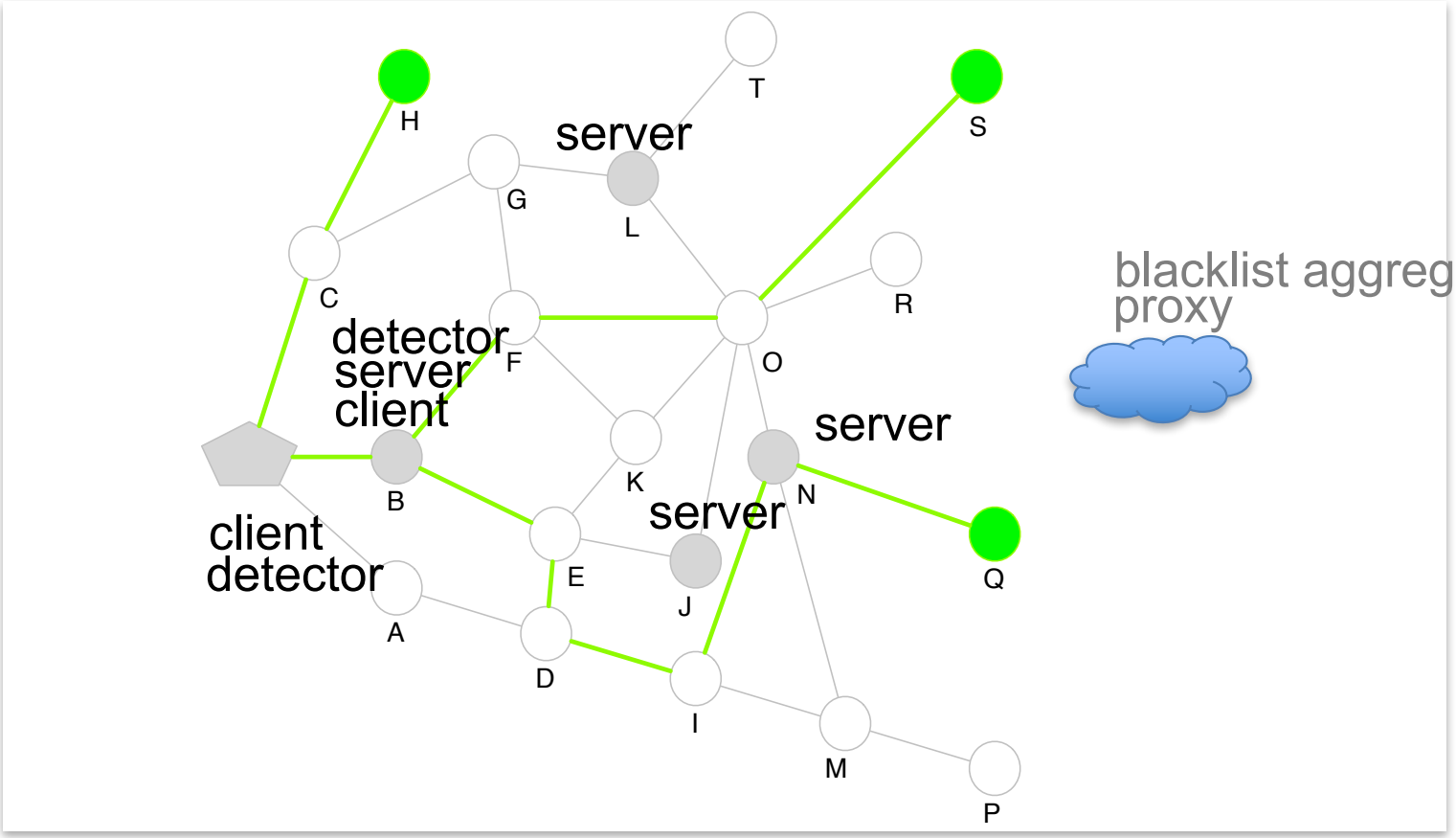
DDoS Attacks: Large and Powerful

- DDoS attacks are increasing in volume and frequency (new record 1.2 Tbps)
- Disproportionate power in hands of attacker
  - Attacks that bring down large, well provisioned victims often wielded by a single person or small group (Spamhouse, Dyn, OVH and Krebs)
  - No special experience or circumstance
  - Cheap for attacker, very expensive for the victim
- Enabled by large, distributed botnets
  - No single entity (centralized or distributed) can withstand this, distributed defenses a must

Our solution: SENSS

- Fully software solution – easy to deploy
- Enables any ISP to offer automated services for DDoS diagnosis and mitigation
  - Naturally distributed, secure, robust to misbehavior
  - Works with existing ISP infrastructure (SDN, Flowspec, Netflow)
- Victim queries its own ISP or remote ISPs
  - About its inbound traffic, routes to its prefixes
  - This helps detect best points for mitigation
- Victim asks select ISPs to:
  - Filter some of its inbound traffic (victim specifies header signature)
  - Demote a route that may contain a bottleneck

SENSS Modules



SENSS APIs at ISPs

- Exposed as Web services
  - Leverage existing functionalities for robustness (replication), security (HTTPS), charging (e-commerce)

Type	Fields	Action/Reply
Traffic query	Flow, dir, obs_time	List of <tag, dir, volume>
Traffic filter/allow	Flow, dir, tag, duration	Deploy filter/allow actions
Route query	Prefix	List of best paths to prefix
Route demote	Prefix, segment, duration	Demote routes with given segment

- Message authentication: Proof of authority for a prefix
  - E.g., RPKI, a DB of known customers, prefixes and public keys
- TLS for communication security

How Can You Help?

- Deploy a passive module:
  - Detector – learn how often you experience DDoS or participate in it
  - Blacklist aggregator – get our feed of suspicious prefixes
- Deploy an active module:
  - Server – automate filter rule deployment in multiple switches
  - Client + Detector – leverage your ISP's DDoS solution and trigger it automatically
- Looking for:
  - Experiences from trenches, what do you do now for DoS?
  - One-time feedback on needs, deployability, concerns
  - 1h/month ongoing feedback from ops world
  - Sites to pilot our solutions

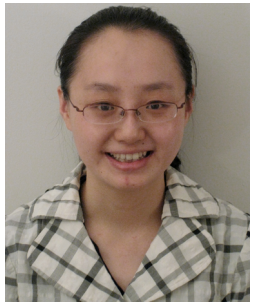
USC University of Southern California

Contact us

sunshine@isi.edu

http://steel.isi.edu/Projects/SENSS/

Jelena Mirkovic



Minlan Yu

Ying Zhang

Sivaram Ramanathan

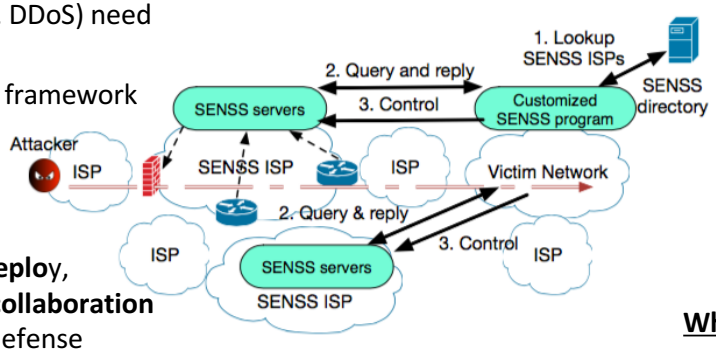
Cybersecurity Research Acceleration
Workshop and Showcase

October 18, 2017 | San Francisco, CA

Quad Chart for: SENSS: Security Service for the Internet

Challenge:

- Distributed attacks (e.g. DDoS) need distributed solutions
- Today's internet has no framework for automated inter-ISP collaboration



Solution:

- SENSS offers **easy to deplo**y, **effective, automated collaboration mechanism** for DDoS defense
- **ISPs** deploy SENSS servers, receive messages from clients, provide monitoring or filtering
- **Edge networks** deploy SENSS clients, detect attacks, devise signatures and decide which actions are needed by which SENSS servers
- All communication is secured from eavesdropping or impersonation
- Clients can only influence their own incoming traffic

Value proposition:

- Increase ISP offering in DDoS defense at zero equipment/software cost
- Solution where attack victim has full control over mitigation and can measure its impact
- Foundation for inter-ISP collaboration

What we need to TTP

- Opportunities to pilot the research
- Feedback on features to support
- Feedback and discussion on ISP concerns

DHS DDoSD #D15PC00184
USC/Yale
PI: Jelena Mirkovic, USC and Minlan Yu, Yale
Team: Sivaram Ramanathan, Ameya Hanamsagar, Davut Yavuz, Goran Scuric, Ying Zhang

Contact us

- mirkovic@isi.edu
- minlanyu@yale.edu

Survey Tools to Collect Feedback

Workshop Overall:
http://bit.ly/ttptechexws

Researcher Assets:
http://bit.ly/ttptechexresearch

Cybersecurity Research Panel: Internet of Things

HomeSHARE - Home-based Smart Health Applications across Research Environments

Blaine Reeder
University of Colorado at Denver

HomeSHARE and Information Security Questions

Blaine Reeder, PhD
Assistant Professor
University of Colorado College of Nursing

College of Nursing
UNIVERSITY OF COLORADO
ANSCHUTZ MEDICAL CAMPUS

College of Nursing
UNIVERSITY OF COLORADO ANSCHUTZ MEDICAL CAMPUS

HomeSHARE: Home-based Smart Health Applications across Research Environments

Blaine Reeder, PhD[2], Kay Connelly, PhD[2], Katie Siek, PhD[2], Kelly Caine, PhD[3], George Demiris, PhD[4], Kamin Whitehouse, PhD[5]
[1]University of Colorado | Anschutz Medical Campus, Aurora, CO; [2]Indiana University, Bloomington, IN; [3]Clemson University, Clemson, SC;
[4]University of Washington, Seattle, WA ; [5]University of Virginia, Charlottesville, VA

Challenge

Lack of smart home and wearable technology research infrastructure prevents investigators from diverse disciplines from answering research questions that can generalize to larger populations.

Researchers typically:

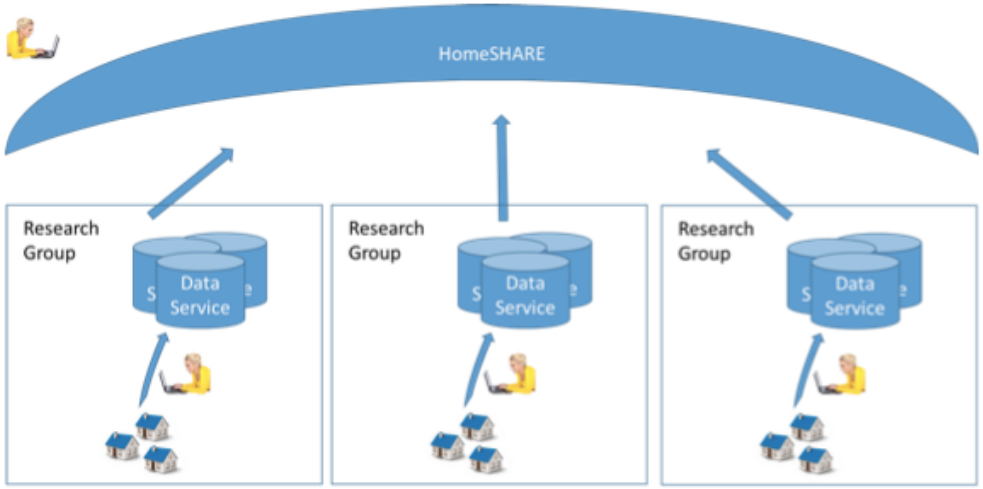
1) Conduct small-scale feasibility studies
2) Recruit participants through convenience sampling
3) Expend substantial resources to build or customize technologies

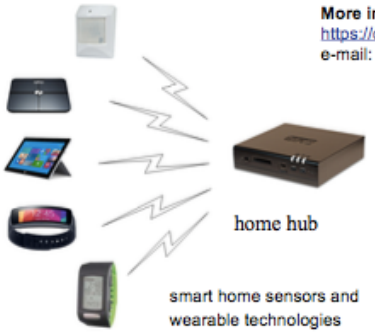
Efforts often:

1) Fail to translate or scale outside their original settings
2) Result in systems that cannot be reused beyond single experiments
3) Miss opportunities to fully capitalize on research dollars

Solution

The Home-based Smart Health Applications across Research Environments (HomeSHARE) initiative is a multi-site collaboration that seeks to develop a geographically distributed smart homes testbed with input from informatics, gerontology, and computer science research communities.





More information:
https://crihomeshare.wordpress.com/
e-mail: blaine.reeder@ucdenver.edu

HomeSHARE sites from East to West
University of Washington, University of Colorado Anschutz, Indiana University, Clemson University, University of Virginia

Value Proposition

- Standardize support for data collected by smart home and wearable devices
- Standardize data collection protocols across research environments
- Provide access to large data sets
- Enable enrollment of more diverse study populations
- Create common governance policies for researchers that cover criteria for participation, shared management responsibilities, and data control/sharing agreements

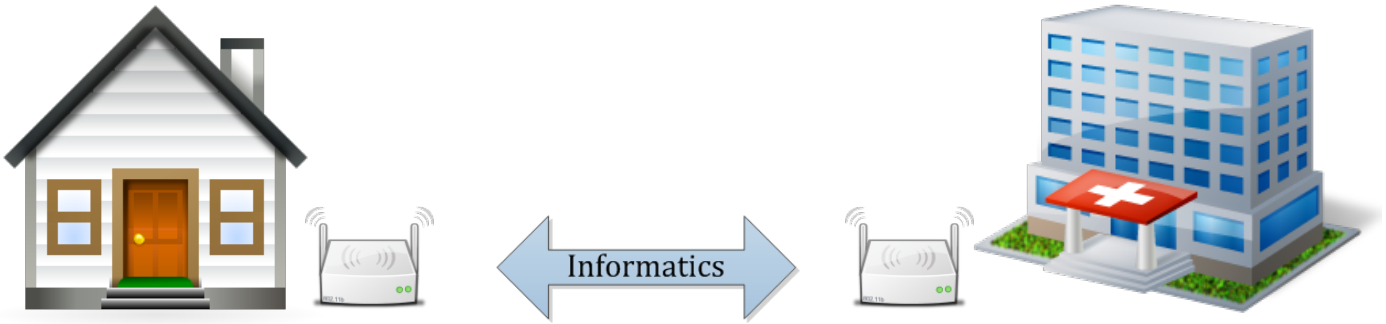
What we need to TPP

- Recommendations for features that HomeSHARE should support
- Data security strategies for smart home and wearable technologies at the device, home hub, and server levels

Acknowledgements

This material is based upon work supported by the National Science Foundation (NSF) under Grant Nos. 1625451 (UW), 1629202 (CU), 1629468 (IU), 1629437 (Clemson). Opinions, findings, conclusions, and recommendations expressed are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Broad Research Goal



Older Adults and
Smart Technologies

Organizations and
Information Systems

College of Nursing
UNIVERSITY OF COLORADO
ANSCHUTZ MEDICAL CAMPUS

Diversity of Devices

1. Installed (“smart home” devices such as motion sensors)




2. Mobile (smart phone, tablets, personal health devices)




3. Wearable (smart watch, activity monitors, smart textiles)




College of Nursing
UNIVERSITY OF COLORADO
ANSCHUTZ MEDICAL CAMPUS

Challenges

- Technology
  - Rapid change
  - Usability
  - Acceptability
  - Abandonment
  - Diversity of devices
  - Battery life
- Data
  - Usefulness
  - Quality (Timeliness, Completeness, Accuracy)
  - Formats
  - Storage and Hosting
  - Security

College of Nursing
UNIVERSITY OF COLORADO
ANSCHUTZ MEDICAL CAMPUS

Information Security Questions

1. How do we manage challenges of siloed data from individual vendors?
   a) Who really owns these data?
   b) What are the implications of a vendor change in data management policy?
   c) Changes in subscriber model?
   d) Changes in ownership/bankruptcy?

2. Is it wise to store device data in clinical data warehouses?
   a) Any personal data merged with health data also becomes health data
   b) These data are then covered by HIPAA

3. What is the best model for a financially sustainable open platform that allows secure data management at the device, home hub, and internet server levels?
   a) Should this platform be HIPAA compliant or should that be handled by a separate system that federates non-health data with clinical data?

Survey Tools to Collect Feedback

Workshop Overall:
http://bit.ly/ttptechexws

Researcher Assets:
http://bit.ly/ttptechexresearch

Cybersecurity Research Panel: Identity & Access Management

Middleware for Certificate-Based Authentication

Kent Seamons
Brigham & Young University

Cybersecurity Research Acceleration Workshop and Showcase

October 18, 2017 | San Francisco, CA

Quad Chart for: TrustBase: Certificate-Based Authentication

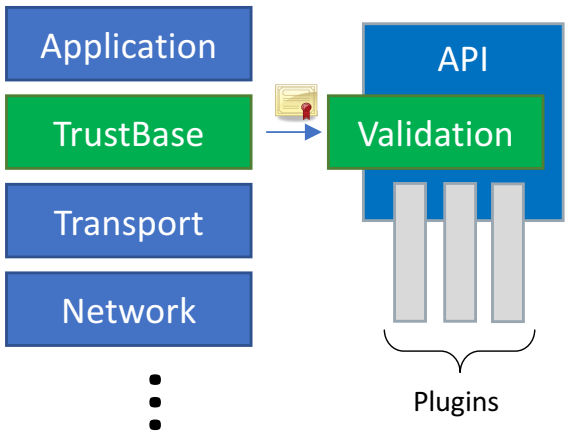
Challenge:

- ❑ Application developers improperly validate website certificates
- ❑ Untrustworthy or coerced Certificate Authorities
- ❑ Alternatives to the system have no common platform for deployment and test

Solution:

- ❑ Authentication as an operating system service
- ❑ Plugins provide flexible deployment of authentication services

Enforcing proper and custom validation of host certificates



Value proposition:

- ❑ All applications will automatically validate certificates correctly
- ❑ Security researchers now have a platform on which to deploy and test certificate authority alternatives

What we need to TTP

- ❑ Your feedback on clients vs middlebox deployment
- ❑ Pilot deployments to gather production data in passive mode

NSF Grant #1528022
PI: Kent Seamons and Daniel Zappala
Computer Science Department
Brigham Young University

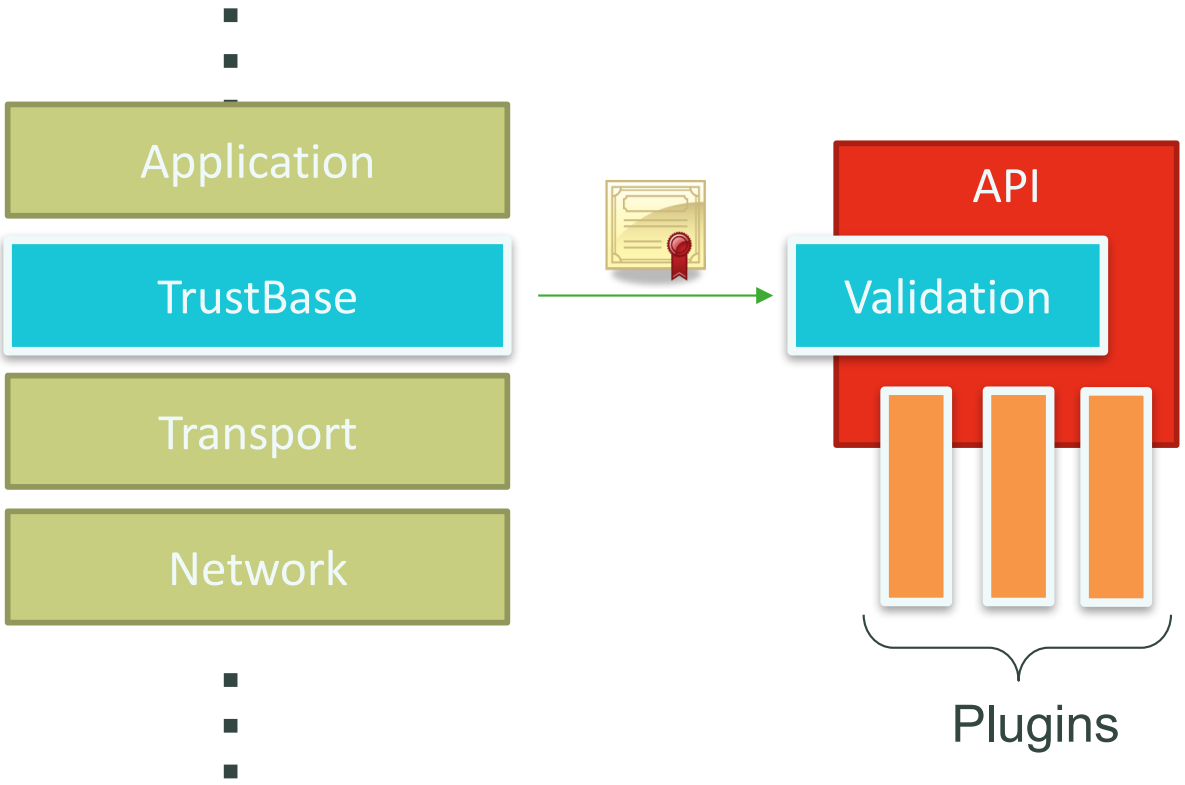
Contact us
seamons@cs.byu.edu
zappala@cs.byu.edu

Problem

- Application developers improperly validate website certificates
- Untrustworthy or coerced Certificate Authorities
- Deployment of alternatives is hard

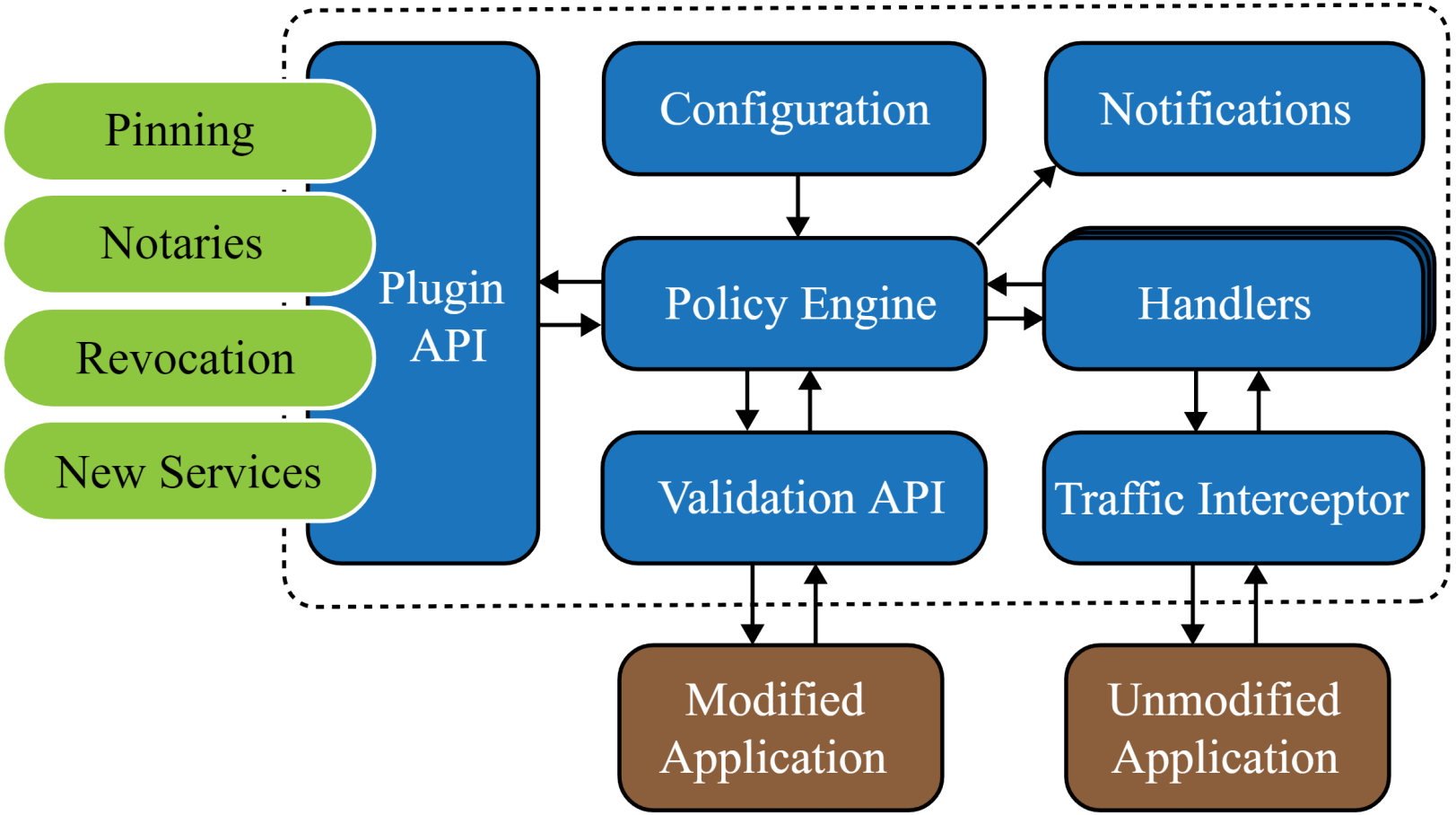
TrustBase

- Motivating principles
  - Centralize authentication as an OS service
  - Empower system admins to dictate how trust decisions are made on their own machines
- Design goals
  - Secure *all* existing applications
  - Prohibit unprivileged applications from acting against administrator rules
  - Provide easy deployment of authentication systems
  - Negligible overhead



Prototypes for

- Linux
- Android (nonrooted)
- Windows


Pinning
Notaries
Revocation
New Services
Plugin API
Configuration
Notifications
Policy Engine
Handlers
Validation API
Traffic Interceptor
Modified Application
Unmodified Application

Feedback

- How best to deploy this technology in the enterprise
- Pilot deployments to gather production data in passive mode

Improving the Security and Usability of Two-Factor Authentication for Cyberinfrastructure

Stanislaw Jarecki
University of California-Irvine

Better Security for Password and Two-Factor Authentication

Stanislaw Jarecki (University of California Irvine)
Nitesh Saxena (University of Alabama Birmingham)

Main collaborators:

Aggelos Kiayas (U Edinburgh)
Hugo Krawczyk (IBM Research)

PhD students on the project:

Maliheh Shirvanian (UA Birmingham)
Jiayu Xu (UC Irvine)

Password (In)Security

- Passwords: **MAIN** authentication tool in the digital era
- Protect our lives and social order, *conveniently* and **Insecurely**

Password (In)Security
Unacceptable State of Affairs

- Attackers routinely compromise servers
  - Steal password-related data
  - Recover user's password via Offline Dictionary Attack
- BILLIONS of passwords stolen
  - MySpace 360M, LinkedIn 165M, eBay 145M,…, Yahoo 3B (!!)
  - … Twitter, RSA, Google, Dropbox, PayPal, Sony, …
- *Current* Two-Factor Authentication schemes do not stop this leakage
  - TFA reduces to 2nd factor (e.g. cell phone) security if password leaks
  - But current TFA's do nothing to protect passwords from leakage

Cryptography Can Help!

- We show ways to strengthen password and two-factor protocols
- Using simple, well-established techniques
  - Mostly blinded Diffie-Hellman [Chaum, Ford-Kaliski, Boyen, …]
- Efficient. Mature. Applicable to the infrastructure used today. **Ready for deployment** in the **real world**.
- Please talk to me if you are interested to learn more (esp. if you see where we can improve, or if you want to transfer this to practice).

Attacks on Password Authentication #1: Offline Dictionary Attack (ODA)

- ODA is the main source of password compromise:
  - *Deadly combination* of human memory limitation (→ low entropy passwords) and server compromise
  - Stealing the "password file" allows testing password guesses against stored hashes; millions++ of password per second (from s/w to dedicated h/w)

Goal: Render these unavoidable exhaustive attacks ineffective!

How: Enforce high-entropy passwords using additional devices/servers

Attacks on Password Authentication #1: Offline Dictionary Attack (ODA)

- ODA is the main source of password compromise

Goal: Render these unavoidable exhaustive attacks ineffective!

How: Enforce high-entropy passwords using additional devices/servers

- What Devices?
  - Cell phone, USB stick: Already used in Two-Factor Authentication!
- What Servers?
  - Can be hosted by any cloud service
  - End-users can utilize it *transparently* to web servers
  - Web servers can utilize it *transparently* to end-users

Attacks on Password and Two-Factor Authentication #2,3,4,…

2. Online dict. attacks (unavoidable): Guess password; try it online.
   - Works w/weak pwds and in targeted attacks (pers. info, sister pwd)
   - 2nd factor helps, but we could do better even here!
3. Phishing/PKI attack: User tricked to send password to the attacker
   - paypa1.com, overwritten links in email, URL-browser manipulation, …
   - Cert signed by rogue CA (do ***you*** know your browser's CA's?)
   - A certificate flagged by the browser but user accepts ("clicking through")
4. Malware on the client (terminal, laptop, phone), e.g. *keyloggers*

Goal: Eliminate, neutralize, or reduce exposure to these attacks

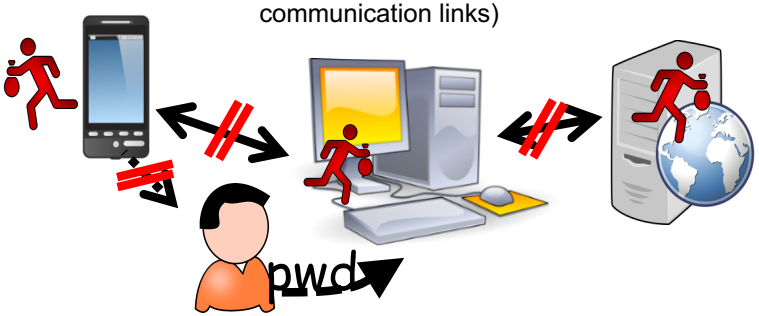
How: Additional devices/servers help, and better cryptography helps!

Better Security for Password and Two-Factor Authentication

Stanislaw Jarecki (UC Irvine), Nitesh Saxena (UA Birmingham)

PASSWORD AUTHENTICATION with 2nd FACTOR

End-to-end security = each component can be compromised: (2nd Factor Device, Client, Server, communication links)



MOTIVATION:

- Password authentication is a *security bottleneck*
- Web services routinely compromised, hashed passwords leak
  → Hackers recover passwords via Offlline Dictionary Attack
- Current Pwd/TFAuth insecure against this (and other attacks)

MAIN OBJECTIVES:

- Achieve end-to-end (maximal) security in all attack scenarios
- Eliminate hashed passwords on servers
  → Protect passwords even if servers are compromised

SECONDARY OBJECTIVES:

- Improve TFA *usability* (e.g. PIN-copying is not necessary)

REQUIREMENTS:

- Browser Extension on Client
- Data-Connectivity on 2nd Factor Device (= Cell Phone)

SOLUTION TECHNIQUES / SPECS:

- Standard Diffie-Hellman, e.g. EC groups, as in TLS/SSL
- Computational cost = 2-3 exp's/party (≈ TLS handshake)

SEVER-TRANSPARENT MODE:

- Client gains strong authentication token from 2nd Factor Device and/or 3rd-party Security Service

CLIENT-TRANSPARENT MODE:

- Server interacts with 3rd-party Security Service

POTENTIAL ADOPTERS:

- *Any internet user*: PwdAuth/TFA transparent to web server
- *Any internet service*: PwdAuth/TFA transparent to end-user

FIST ADOPTERS (PILOTS):

- Internet end-users using 3rd party service
- Educational Institution logon server?
- Industry PwdAuth / TFA providers as partners?

TECHNOLOGY TRANSFER:

- Software libraries will be made available

CONTACT :

- Stanislaw Jarecki, UC Irvine, sjarecki@uci.edu
- Nitesh Saxena, UA Birmingham, saxena@uab.edu

Survey Tools to Collect Feedback

Workshop Overall:
http://bit.ly/ttptechexws

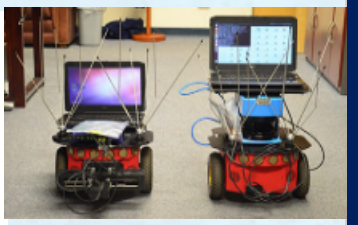
Researcher Assets:
http://bit.ly/ttptechexresearch

Cybersecurity Research Panel: Multidisciplinary Cybersecurity

Capacity building in Cybersecurity-literacy: An inter-disciplinary approach

Shamik Sengupta
University of Nevada, Reno

http://capacity.unr.edu



NSF CyberCorps(R): "Collaborative Research: Capacity Building in Cybersecurity-Literacy: An Inter-Disciplinary Approach"

A partnership between UNR and TMCC

Contact: Dr. Shamik Sengupta (ssengupta@unr.edu) and Dr. Bill Doherty (bdoherty@tmcc.edu)


JURASSIC PARK
An Adventure
65 Million Years In The Making.


Dennis Nedry


Office Space
Work sucks.

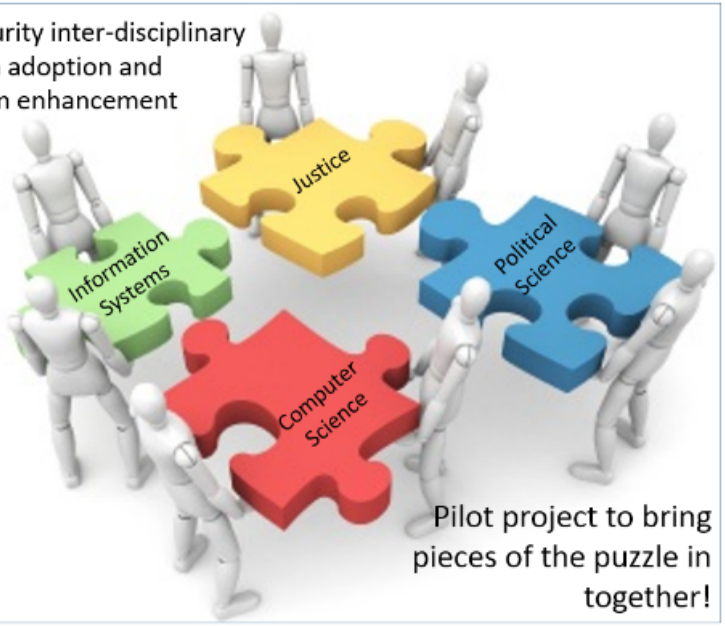

HARRISON FORD
PAUL BETTANY
FIREWALL
EVERYTHING HE LOVES IS ABOUT TO BE USED AGAINST HIM.
FEBRUARY
THEY'RE ALREADY INSIDE.


KEANU REEVES
LAURENCE FISHBURNE
MATRIX


JOHN TRAVOLTA
HUGH JACKMAN
HALLE BERRY
DON CHEADLE
Log on.
Hack in.
Go anywhere.
Steal everything.
SWORD FISH

http://capacity.unr.edu

Cybersecurity inter-disciplinary education adoption and curriculum enhancement



Pilot project to bring pieces of the puzzle in together!

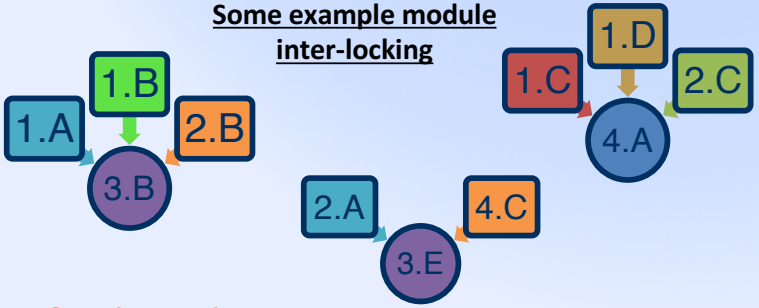
Capacity building in Cybersecurity-literacy: An inter-disciplinary approach

What is the project all about?

The project is based on a partnership between the University of Nevada, Reno (UNR), and the Truckee Meadows Community College (TMCC). By bringing in scholars from multiple disciplines, this project proposes to explore unique ways to engage students in inter-disciplinary cybersecurity education, to sustain long-term research and education partnerships and to motivate students towards protection of cyberspace.

Inter-disciplinary Cybersecurity Capacity Building

Some example module inter-locking



Inter-disciplinary Holistic Cybersecurity

Lib 1: Social Science and Human Factors

- Module A: Information Technology and International Security Policy
- Module B: Cyberwar, Terrorism, Radicalization, and the War of Ideas
- Module C: Human-factor espionage (HUMINT)
- Module D: Political economy of cybersecurity
- Module E: Human cybersecurity

Lib 2: Legal Issues

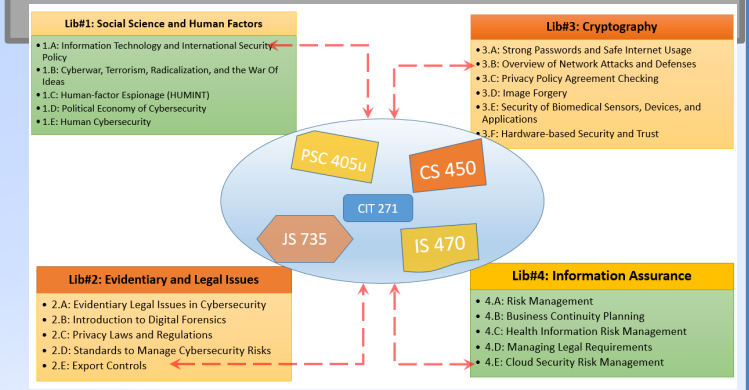
- Module A: Evidentiary Issues in Cybersecurity
- Module B: Introduction to Digital Forensics
- Module C: Privacy Laws and Regulations
- Module D: Standards to Manage Cybersecurity Risks
- Module E: Export Controls

Lib 3: Cryptography Library

- Module A; Strong Passwords and Safe Internet Usage
- Module B: Overview of Network Attacks and Defenses
- Module C: Privacy Policy Agreement Checking
- Module D: Image Forgery
- Module E: Security of Biomedical Sensors, Devices, and Applications
- Module F: Hardware-based Security and Trust:

Lib 4: Information Assurance

- Module A: Risk Management
- Module B: Business Continuity Planning
- Module C: Health-Information Risk-Management
- Module D: Managing Legal Requirements
- Module E: Cloud Security Risk Management



An example of four modules fused and adopted with appropriate intensity into different target courses

"This work is supported by the National Science Foundation under Grant #1516724."

Capacity.unr.edu

General Module Design Goals

- Class content for between 1.5 and 6 hours to allow adaptation for one class period or up to two weeks of class
- Content appropriate for beginning, intermediate and graduate level students
  - Presentations, readings and activities can be adjusted based on student population and instructor comfort level.
- Live training options as well as support discussion forums

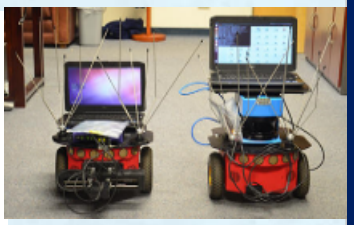
Questions?

Dr. Shamik Sengupta (ssengupta@unr.edu)

Website: http://capacity.unr.edu/

Establishing market based mechanisms for CYBer security information Exchange (CYBEX)

Shamik Sengupta
University of Nevada, Reno



Establishing market based mechanisms for CYBer security information EXchange (CYBEX)

Contact: Dr. Shamik Sengupta (ssengupta@unr.edu)

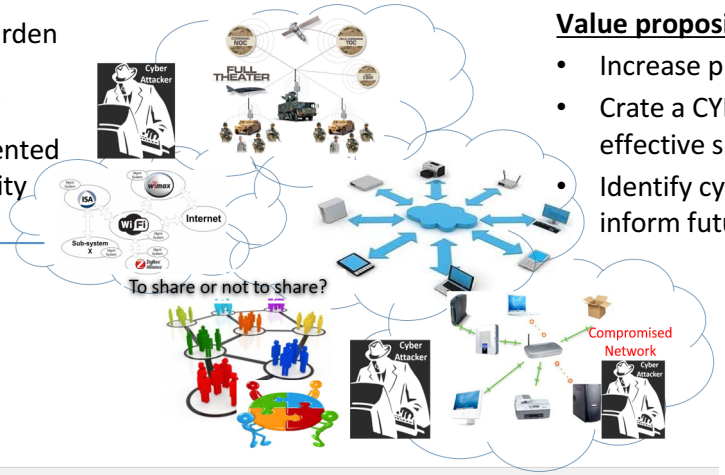
Cybersecurity Research Acceleration Workshop and Showcase

October 18, 2017 | San Francisco, CA

Quad Chart for: SATC: Establishing market based mechanisms for CYBer security information EXchange (CYBEX)

Challenge:

- Can CYBEX help us share the burden of cybersecurity?
- Understanding the Necessity of cyberinsurance and market oriented approach for better cybersecurity information utilization



Value proposition:

- Increase proactive cybersecurity
- Crate a CYBEX framework for effective sharing
- Identify cybersecurity needs to inform future research

Solution:

- **Establish** market based game theoretic mechanisms
- **Identify, model and analyze** the conflicts
- **Leverage** evolutionary and adaptive game theory to understand the dynamics
- **Investigate** the necessity of cyberinsurance and market oriented approach for better cybersecurity information utilization

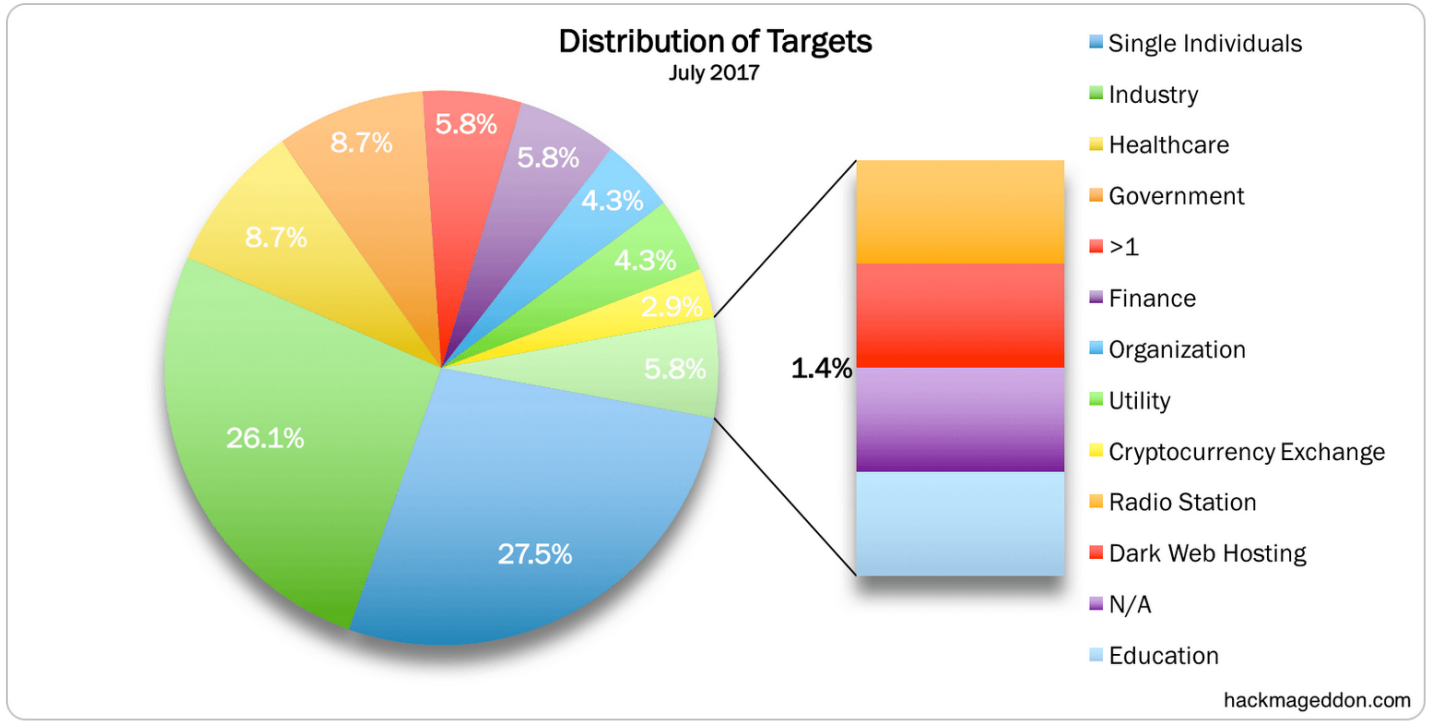
NSF SATC #TBD
CYBEX
PI: Shamik Sengupta, Executive Director
UNR Cybersecurity Center

What we need to TTP

- Your feedback
- Opportunities to pilot the research

Contact us

- ssengupta@unr.edu

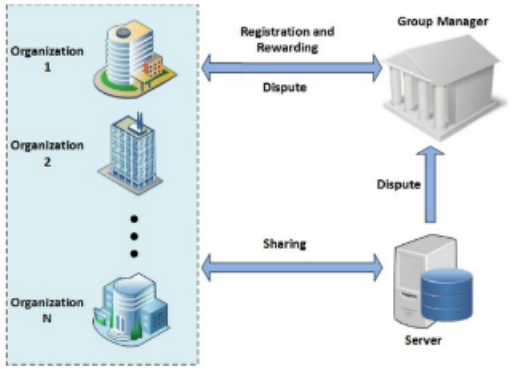


Source: http://www.hackmageddon.com/2017/08/24/july-2017-cyber-attacks-statistics/

CYBEX

- A framework to provide a service of structured information exchange about measurable security states of systems together with incidents stemming from cyber attacks.
- Benefits:
  - (1) fostering cyber situational awareness,
  - (2) developing proactive defense mechanisms,
  - (3) clarity in understanding the threat landscape, malicious actors, security loopholes etc.
- Challenges:
  - (1) the possibility of information exploitation through such exchange as the sharing organizations may not trust on the other participants,
  - (2) organizations' market reputation might get negatively affected,
  - (3) lack of incentivization with respect to a organization's sharing contribution.

CYBEX



Game Formulation

	Participate & Share	Not Participate
Participate & Share	$Sa\log(1+I)-x-c,$ $Sa\log(1+I)-x-c$	$a\log(1+I)-x-c,$ $a\log(1+I)$
Not Participate	$a\log(1+I),$ $a\log(1+I)-x-c$	$a\log(1+I),$ $a\log(1+I)$

I – amount of investment made by the firms
a - simple scaling parameter that maps user satisfaction/benefit to a dimension equitable to the price/monitory value
c - cost of participation in the CYBEX framework
S – Scaling benefits of sharing

Cyber-Insurance

•Cyber-insurance as a CYBEX model incentive:

•Insurance incentives can be used to motivate socially optimal sharing behavior and deter harmful behaviors. If cyber-insurance is added as an incentive in exchange for information sharing, firms benefit due to efficient and reliable risk management using cyber-insurance. On the other hand, supply side gets benefited by obtaining information they need.

•Modelling Cyber-Insurance with information sharing framework:

•Cyber-insurance can be modelled in such a way that the coverage and premium for the insurance will depend on the sharing level, frequency of attacks and attack severity level. As the frequency of attack increases the premium for the insurance gets incremented compared to previous, however periodically the premium amount decreases on how successfully the network strives against cyber attacks for long with the help of cooperation.

•Challenges in modelling Cyber-Insurance:

•**1)Information Asymmetry:** Insurers not being able to classify the nodes due to the lack of information such as security levels opted by the firm, attack frequencies. Often, firms do not wish to share the data due to privacy issues and also due to the concern of reputation loss.

•**2)Non-Linearity:** Risk domain for cyber security can be said as non-linear, meaning, that same attack can cause either small or big losses in different occasions.

•**3)Correlated risks:** Due to the interdependent nature of the networks, security compromises can arise from the failure of security of independently owned systems to contribute to overall prevention

Questions?

Dr. Shamik Sengupta (ssengupta@unr.edu)

Website: https://www.cse.unr.edu/~shamik/

University of Nevada, Reno

A National Tier 1 University

Survey Tools to Collect Feedback

Workshop Overall:
http://bit.ly/ttptechexws

Researcher Assets:
http://bit.ly/ttptechexresearch

Closing

Florence Hudson
SVP and Chief Innovation Officer, Internet2

Survey Tools to Collect Feedback

Workshop Overall:
http://bit.ly/ttptechexws

Researcher Assets:
http://bit.ly/ttptechexresearch

CINC UP: CYBERSECURITY RESEARCH ACCELERATION WORKSHOP AND SHOWCASE

Brought to you by CENIC and Internet2

JOHN DUNDAS
VP and CTO, CENIC

FLORENCE HUDSON
SVP & Chief Innovation Officer, Internet2