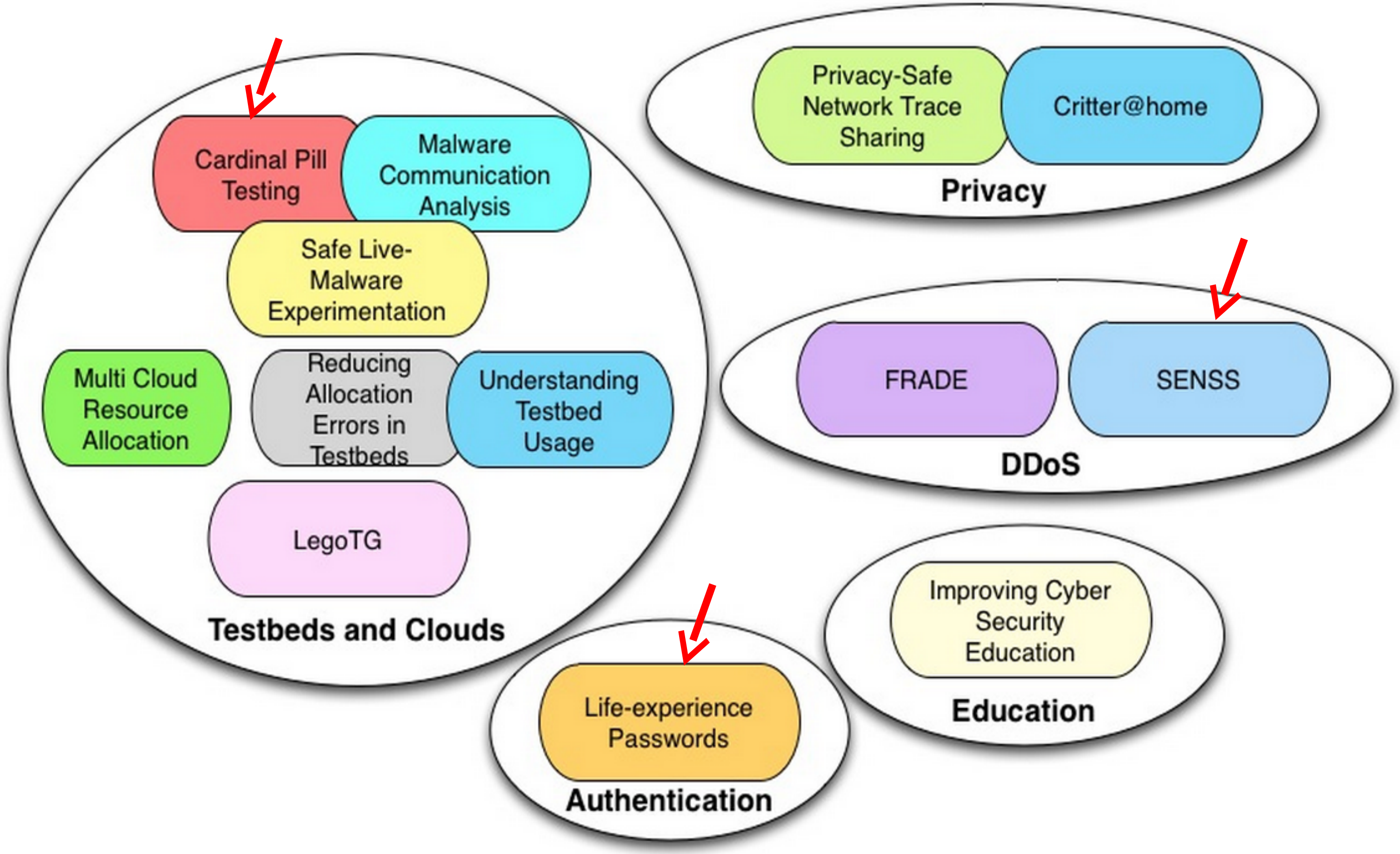
STEEL Lab

Prof. Jelena Mirkovic, USC/ISI
sunshine@isi.edu

Our Research Projects



Testbeds and Clouds

Cardinal Pill Testing

Malware Communication Analysis

Safe Live-Malware Experimentation

Multi Cloud Resource Allocation

Reducing Allocation Errors in Testbeds

Understanding Testbed Usage

LegoTG

Privacy

Privacy-Safe Network Trace Sharing

Critter@home

DDoS

FRADE

SENSS

Authentication

Life-experience Passwords

Education

Improving Cyber Security Education

Cardinal Pill Testing

- Malware analysis requires VMs and debuggers
  - To understand malware’s functionality
  - To recover quickly from failures
- Environment-sensitive malware detects VMs and debuggers and stops working
- Detection (VM/debugger vs PM):
  - Using semantic differences in execution (same command, same inputs, different outcomes)
    - command + inputs = pill
  - Using strings/labels in OS left by VM/debugger
  - Using timing (VM/debugger is slower)

Cardinal Pill Testing

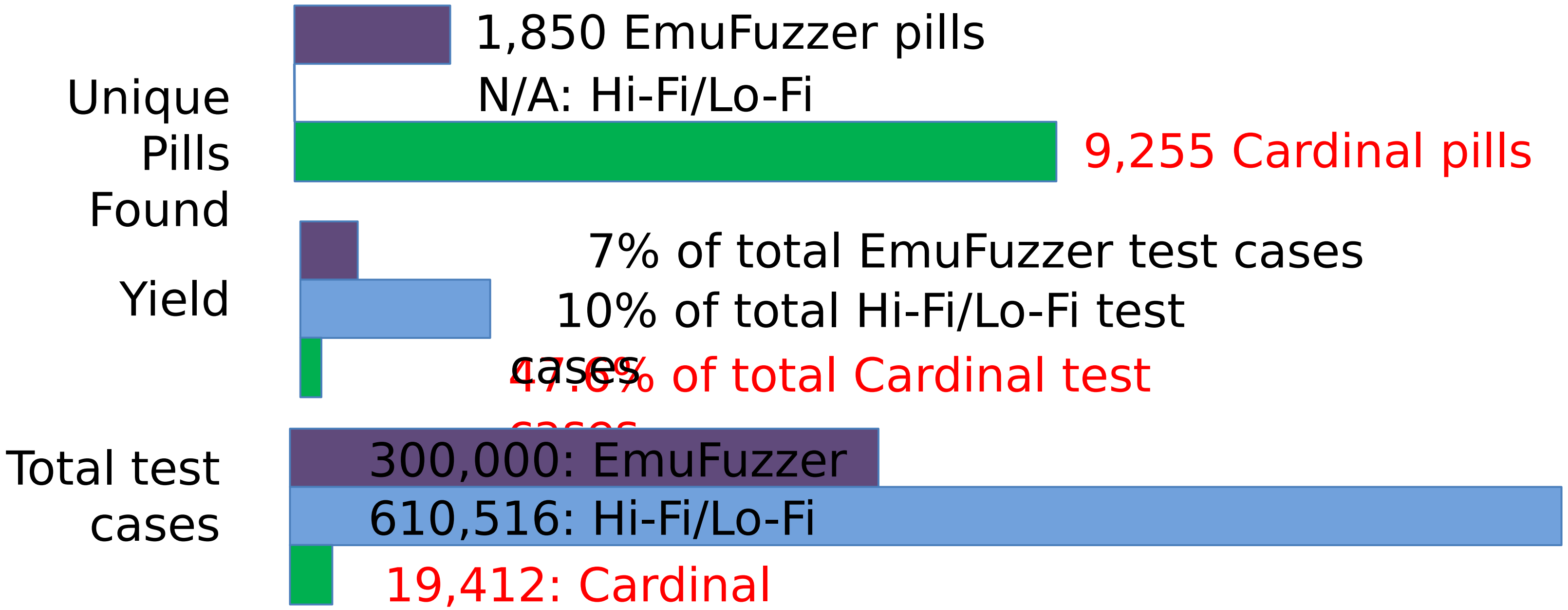
- Can we enumerate diffs between VMs and PMs?
  - Hide them by serving the right response to malware
  - Focus on semantic differences (the rest is easy)
- How to enumerate w/o exhaustive testing of inputs?
  - Group commands by functionality
    - 1,653 instr □230 partitions
  - Understand semantics of each group, test min, max, random and boundary values of parameters
  - Run the same command+inputs in VM and PM, record all state (memory, registers, exceptions)
    - If different, we found a pill

Cardinal Pill Testing

- E.g. **aaa**, **aas**, **daa**, and **das**
  - Compare the **al** register with **0fh** and check the adjustment flag **AF**
- Test cases for this partition
  - Initialize **al** to min (**00**), max (**ff**), boundary (**0f**), random values in different ranges ([**01**, **0e**], [**10**, **fe**])

Cardinal Pill Testing

Results, compared to two related works



Life-Experience Passwords

- Memorable passwords are easily guessed
- Strong passwords are reused and easily forgotten
- Non-textual passwords have similar problems
- People don’t easily retain new memories
  - “Human memory is fundamentally associative, meaning that a new piece of information is remembered better if it can be associated with previously acquired knowledge that is already firmly anchored in memory. The more personally meaningful the association, the more effective the encoding and consolidation … On the other hand, information that a person finds difficult to understand … will usually be poorly remembered, and may even be remembered in a distorted form”

    http://www.human-memory.net/

Life-Experience Passwords

- Use existing life experiences to create a password
  - Memories about events (wedding, graduation), trips, people, places, learning
- Select an experience, supply several facts
  - When, where, who, activities, conversations
- We extract Q & A from this, and a title
  - Title and Questions become prompts for authentication
  - Answers become LEP (life-experience password)
- More memorable and diverse than passwords
- Harder to guess/mine than security questions:
  - Some facts can be guessed/mined but not all

Life-Experience Passwords

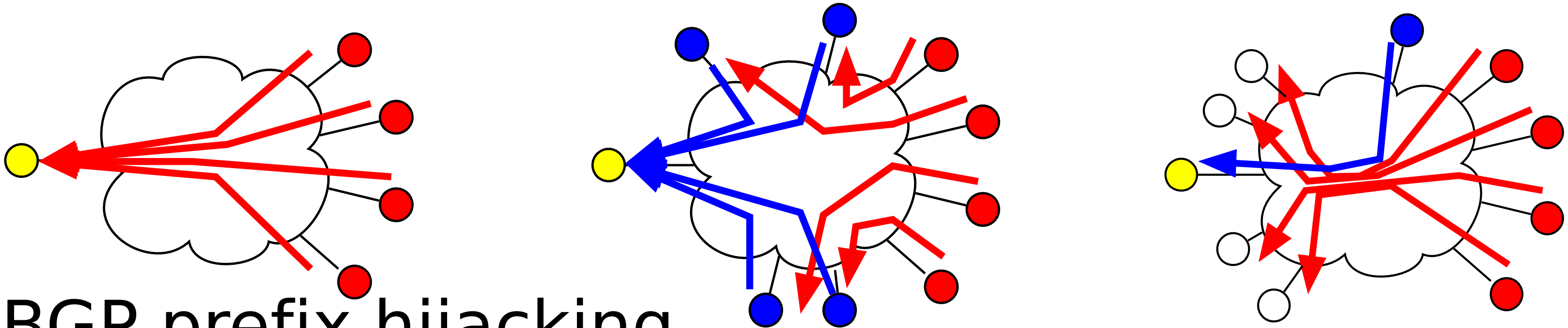
Pilot study with 61 MTurk and USC students

- **Security:** 80% of generated LEPs have higher strength than 3class8 passwords.
- **Memorability:** 72% of users can successfully authenticate with a LEP, vs 30% with an ordinary password.
- **Diversity:** 2.2% of LEPs were duplicate, vs 13.3% of ordinary passwords
- **Guessability:** 5% of LEPs can be guessed vs 22% of ordinary passwords.
- **User burden:** A few minutes to create, a minute to authenticate

SENSS

Growing DDoS and prefix hijacking attacks

DDoS



BGP prefix hijacking

- Annouce V’s prefix (origin) or short AS path (closeness)
- Blackholing (drop traffic) or interception (sniff or modify forward to V)

SENSS

The best locations for diagnosis and mitigation are often far from the victim

- Victim cannot observe nor control traffic and routes at these locations

Example: Crossfire

- Congested link outside the victim’s network
- ISP does not see anomalies; many srcs/dsts in attack

Example: Prefix hijacking

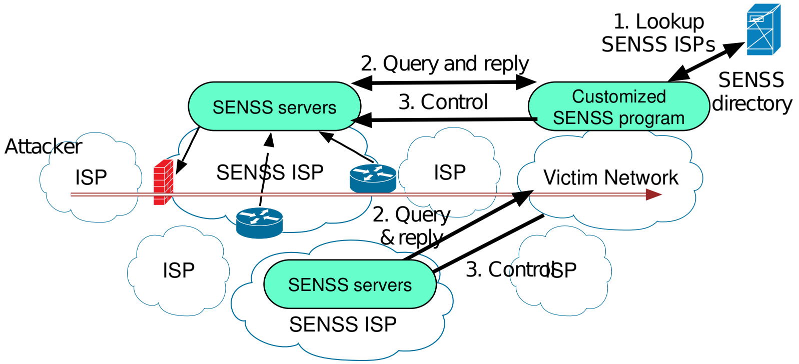
- Networks far from victim accept and propagate route

Mitigation should involve remote ISPs

- Today: sustaining attacks not fixing the problems

SENSS

- Victim identifies ISPs to interact with using public SENSS director
  - Sends to each a query



- ISPs authenticate prefix ownership, process query, charge the victim and return replies

- Victim decides which control actions to apply and where
  - Sends messages about this to chosen ISPs

- ISPs authenticate prefix ownership, charge the victim, implement requested actions

SENSS

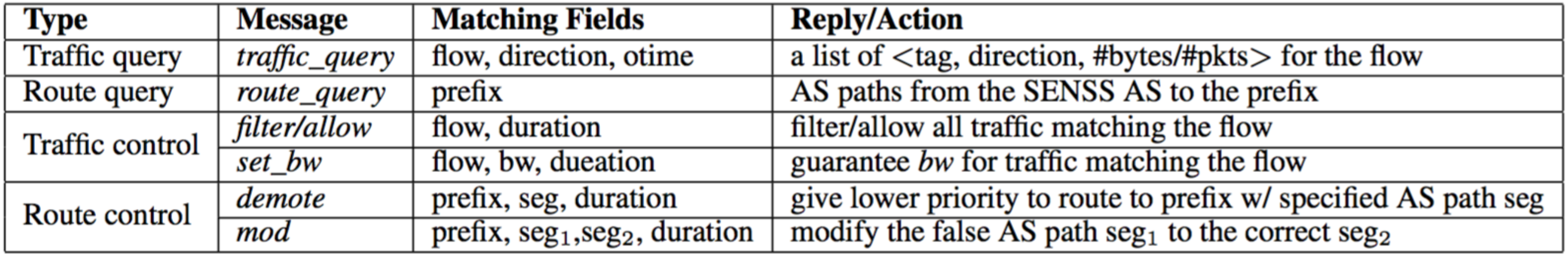
1. Simple actions at ISPs, intelligence at victim
2. Direct victim-remote ISP communication

Benefits

- Incentives for ISPs (easy implementation)
- Efficiency in sparse deployment
- Robustness to misbehavior
- Custom and evolvable attack handling

SENSS

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



Type	**Message**	**Matching Fields**	**Reply/Action**
Traffic query	*traffic_query*	flow, direction, otime	a list of <tag, direction, #bytes/#pkts> for the flow
Route query	*route_query*	prefix	AS paths from the SENSS AS to the prefix
Traffic control	*filter/allow*	flow, duration	filter/allow all traffic matching the flow
	set_bw	flow, bw, dueation	guarantee *bw* for traffic matching the flow
Route control	*demote*	prefix, seg, duration	give lower priority to route to prefix w/ specified AS path seg
	mod	prefix, seg_1,seg_2, duration	modify the false AS path seg_1 to the correct seg_2

Tag = neighbor’s AS number (+ geolocation)

SENSS

RPKI to verify prefix ownership

TLS for communication security

Enabling communication during attacks

- Victim may be flooded or its prefixes hijacked
  - Cannot receive replies, may not be able to send messages
- Offload victim functionality to a proxy in another network
  - Use ROA to delegate prefix ownership
  - May set up proxies as backup service
  - Proxy monitors the victim operation, turns on

SENSS

- Simulation results on AS topology
  - Adoption in 20 large ISPs
  - Eliminate 80-96% DDoS attack traffic
  - Correct 92–99% of polluted ASes for BGP prefix hijacking
- Deployment on random selection of ASes
  - Helps customers of these ASes with some flavors of DDoS attacks (w/sig, reflection)
  - Wider deployment helps extend the benefits to remote customers and for more attacks
    - Especially deployment on well-connected Tier 2

Thank You

- For more info:
  - http://steel.isi.edu
  - http://www.isi.edu/~mirkovic
  - sunshine@isi.edu