Florida Institute of Technology
Harris Institute for Assured Information

GENI Ideas: Instrumentation, Experiments and Security

Richard Ford (rford@fit.edu)
Ronda Henning (rhenning@harris.com)

Three ideas, One slide…

- GENI Ideas: Instrumentation, Experiments and Security

  Richard Ford (rford@fit.edu)
  Ronda Henning (rhenning@harris.com)

- Three Ideas: Monitoring
  - Develop a unified, modular monitoring protocol for GENI nodes
    - Single set of APIs implemented on each platform at the virtualization layer
    - Backplane logging channel required
    - Modular logging allows for maximum reuse of code
    - Logging should not change the results… but how will we know?
    - No real "opt in" for external users (those running outside GENI slices) whose data we will be snarfing
    - BTW, this is going to generate a LOT of data…
    - GENI enablement of campus environments: how to adhere to campus policies (for example, RIAA-related issues)
    - Privacy, privacy, privacy, privacy… oh, and privacy
      - As AOL release taught us, pseudonymity is of little help
- Experiments
  - Malware…
    - Per Nick: write a viable worm and he will mutilate you in interesting novel ways!
    - Do need to ensure containment of effect (spread too obviously, but there's no excuse)
      - See my comment on monitoring previously
    - Desperate need for background traffic – experimentation without this is meaningless
      - Furthermore, should follow the type of extremes we see in reality
      - Don't require experimenters to be experts in this!
      - Replay of stored traffic is okay, but it's unclean and doesn't reflect some very interesting environments (like MANETs)
    - How will we get users to "opt in" to these experiments?
      - And opt in to the monitoring we'll need
- Security
  - Statefulness is (often) the enemy of security
    - Reducing saved state of GENI between and during runs narrows the window for an attacker
  - What stops a cluster owner stealing IP from experimenters?
    - Where cluster owner could be, for example, a hostile government…
  - What happens when GENI gets used for evil (be a great target for a botherder, for example…)
    - Should be rate limits and heuristics at the GENI/Internet border that can shutdown a slice… but this is HUGELY double-edged
    - Need a federated, distributed framework for detection
    - Outliers are really the interesting parts in many experiments we shouldn't shut these down "accidently"
    - What stops an experimenter (or someone posing as an experimenter) deploying hostile code to user nodes?
- Contact
  - Richard: rford@fit.edu
  - Ronda: rhenning@harris.com

Florida Institute of Technology
Harris Institute for Assured Information

Monitoring

- Must develop a unified, modular monitoring protocol for GENI nodes
  - Single set of APIs implemented on each platform at the virtualization layer
    - For example, system API logging… solve generic problem and configure
  - Backplane logging channel required
  - Modular logging allows for maximum reuse of code
    - … rolled up per slice
  - Logging should not change the results… but how will we know?
  - No real "opt in" for external users (those running outside GENI slices) whose data we will be snarfing
  - BTW, this is going to generate a LOT of data…
  - GENI enablement of campus environments: how to adhere to campus policies (for example, RIAA-related issues)
    - Flexibility of demarq points?
  - Privacy, privacy, privacy, privacy… oh, and privacy
    - As AOL release taught us, pseudonymity is of little help

Experiments

- Malware…
  - Per Nick: write a viable worm and he will mutilate you in interesting novel ways! (Must check with IRB)
  - Do need to ensure containment of effect (spread too obviously, but there's no excuse)
    - See my comment on monitoring previously
  - Desperate need for *good* background traffic – experimentation without this is meaningless
    - Furthermore, should follow the type of extremes we see in reality
    - Don't require experimenters to be experts in this (allow as bolt on)
    - Replay of stored traffic is okay, but it's unclean and doesn't reflect some very interesting environments (like MANETs)
  - How will we get users to "opt in" to these experiments?
    - And to opt in to the monitoring we'll need

Security

- Statefulness is (often) the enemy of security
  - Reducing saved state of GENI between and during runs narrows the window for an attacker
- What stops a cluster owner stealing IP from experimenters?
  - Where cluster owner could be, for example, a hostile government…
- What happens when GENI gets used for evil (be a great target for a botherder, for example…)
  - Should be rate limits and heuristics at the GENI/Internet border that can shutdown a slice… but this is HUGELY double-edged
  - Need a federated, distributed framework for detection (ties back to monitoring)
  - Outliers are really the interesting parts in many experiments we shouldn't shut these down "accidently"
  - What stops an experimenter (or someone posing as an experimenter) deploying hostile code to user nodes?

Florida Institute of Technology
Harris Institute for Assured Information

Contact

- Richard: rford@fit.edu
- Ronda: rhenning@harris.com

Florida Institute of Technology
Harris Institute for Assured Information