Report from GENI Day 1

The Participants of the Security Breakout Sessions

Who We Are

- ✓ Terry Benzel
- ✓ Matt Bishop
- ✓ Roy Campbell
- ✓ Hao Chen
- ✓ Chen-Nee Chuah
- ✓ Anupam Datta
- ✓ Wu-Chang Feng
- ✓ Deb Frincke
- ✓ Toru Hasegaw
- ✓ Dijiang Huang
- ✓ Cynthia Irvine
- ✓ Eunjin (EJ) Jung
- ✓ Himanshu Khurana
- ✓ Karl Levitt
- ✓ Steve Liu
- ✓ Charles P. Meister
- ✓ John Mitchell
- ✓ Arnab Roy
- ✓ John Wroclawski

Four Questions

- What security experiments would we run?
- What capabilities do we need from GENI in order to run them?
- What sort of security should be designed into GENI's design, implementation and operations?
- What questions do we have for NSF?

Themes for Capabilities and Security Needs of GENI itself

- Functional Requirements
  - Authentication, Auditing, Monitoring
- Assurance Requirements
  - First thing to do: decide what level of assurance is needed
  - Trusted path/trusted channel
- Confinement/Separation
  - We need it ☺
  - To keep experiments isolated from one another, keep them within GENI, and protect the GENI platform
  - Biological or disease models for “high risk” experimental facilities

More Themes

- Usability/Human Factors
  - Interface to security mechanisms should be intuitive and simple
  - Mindfulness of differing user domains
- Monitoring/Detection
  - Audit trails, protection of audit trail, tools for inspection
  - Requesting certain levels of audit
- Privacy and Confidentiality
  - Who has access to the audit data? Legal and law enforcement?
  - What would we put in a privacy toolkit or API?
  - How will we protect experiments and experimental data?

Still More Themes

- Operational policy
  - Assumptions about maintenance, “good citizenship” …
  - Real-time working group should consider the effects of security upgrades or auditing level changes on validity of timing results
- Physical security of GENI components
  - Assumptions about (lack of) national or natural disasters
  - The “insider problem” again

Experiments

- Simulation of critical infrastructure, for example SCADA and power networks in general
- Large scale (very large scale) attacks, such as worms or botnets
- Disaster simulation and recovery
- Traceback
- Social experimentation – acceptability of security
- Performance and metrics
- Policy experiments – dynamic policies, adaptive policies, heterogeneous policy composition

Questions for NSF

- What might the GENI security architecture look like?
- How will this Town Hall meeting influence it?
- What do we mean by security being “good enough”?
- Is GENI a prototype of the future Internet?
- What is the plan for operational security in GENI? How does that mesh with the plan for operations?
- How will GENI enable users to comply with regulatory policies?
- What security toolkits and interfaces can be provided for the experimenter so that we can make the lives of the experimenters easy with respect to security?

GENI Security Architecture

- ✓ Open architecture so things can be rolled into GENI over time
- ✓ Distributed TCB functioning as a slice separator with assured channels between slices (“trusted and trustworthy”)
- ✓ A plan or philosophy to articulate a distributed TCB for composition
- ✓ Needs to be a process throughout the lifetime of GENI, using a paradigm to ensure security is built into the process

What Is “Good Enough”?

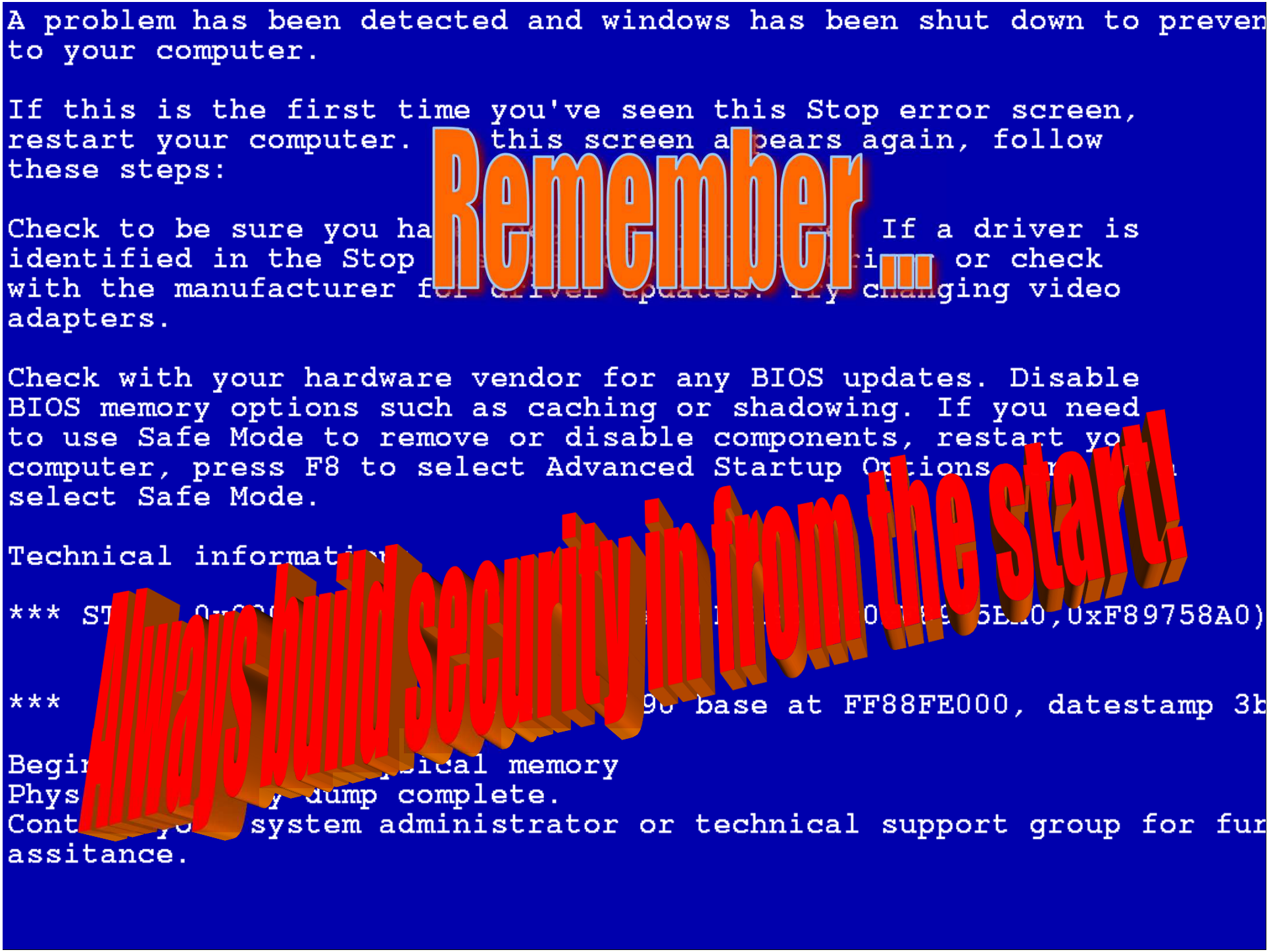
- Mission- and experiment- driven
- One possible aproach to answer this:
  - How much is security needed to run non-security experiment?
  - Then … how much security is needed to run security experiments?
- Note legal/regulatory obligations, also
- An ongoing conversation

Security Toolkits and Interfaces

- How will GENI support tech transfer (making the tools and technologies available for researchers to use in building their own experiments)?
- Will GENI support naïve users, for instance, social scientists using GENI in conjunction with computer scientists?
- Will GENI provide a policy specification language that makes policies easy for users to express, and can be (formally or informally) verified to meet the users' security goals?

Operational Security

- Use GENI slices reserved to watch over GENI slice (trusted and trustworthy slice)
- What is provided in that slice grows with time (begin with clock, then add more ...)
- As GENI is a federated process, develop agreements to be signed for baseline security and incident response plan to be in place almost as soon as GENI is deployed; this must also handle small orgs/single user nodes


A problem has been detected and windows has been shut down to preven
to your computer.
If this is the first time you've seen this Stop error screen,
restart your computer.
these steps:
Check to be sure you ha
identified in the Stop
with the manufacturer f
adapters.
Check with your hardware vendor for any BIOS updates. Disable
BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart yo
computer, press F8 to select Advanced Startup Options
select Safe Mode.
Technical informat
*** ST
*** base at FF88FE000, datestamp 3b
Begi
Phys
Cont
assitance.
Remember...
Always build security in from the start!