Trustworthy Host Platforms For Accelerated Research And Education: Strategic Cyber Threat Reduction Through International Research Cooperation

John C. Mallery
Computer Science & Artificial Intelligence Laboratory
Massachusetts Institute of Technology

Abstract: The deepening world-wide cyber insecurity crisis is destabilizing traditional international security architectures. Funding by government research agencies can shift the balance from offense toward defense dominance by raising assurance globally across the information and communication technology fabric. Such a strategy can be implemented via research programs to create open-source high assurance reference platforms for host computers and networking components that will accelerate research, education, and adoption by industry. Beyond capacity building and research productivity, an important objective is to spread lower risk technologies around the world in order to raise the difficulty for malicious actors to engage in cyber crime, espionage and attacks. This approach implements cyber arms control not by unverifiable and unlikely international treaties but rather by raising the assurance level of systems globally and pervasively so as to eliminate lower difficulty penetration vectors and privilege escalation techniques, and thereby, constrain cyber offense. As the information technology capital goods industry is incentivized to meet or exceed the assurance levels in the open source world, n this way, a negative feedback cycle can be initiated that reduces cyber instability. To incentivize adoption, the proposed research program emphasizes high agility tool chains designed for verifiability, modularity, collaboration, and evolution as a means to lower development costs through higher productivity.

Presentation in the panel entitled “Policy, Ethics, and International Collaboration” at *The BIC/DIMACS/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics* in The Cloud, Malaga, Spain, June 7, 2013.

Version: 8/12/13 11:03

Summary

- Cyber insecurity crisis is deepening
  - Pol-mil interaction with cyber
  - Offense as defense is highly unstable
- Cyber arms control = raising assurance of COTs host
  - Wide adoption necessary for stabilizing impact
- Reference secure host research platforms enable:
  - Accelerated IA research and education
  - Increased trustworthiness of open source supply chain
  - Improved minimum IA best practices for commercial sector
  - Elimination of lower end attack vectors
- Propose funding by research agencies for shared host platforms that include:
  - Verifiable system program language
  - High assurance operating systems & HW ISAs
  - Persistent transactional memory
  - Intelligent development environments
- Incentivize industry
  - Technology inject to open source world
  - Flood markets with high assurance host stack
  - Lower investment risk to best current engineering
  - Raise level of commercial host security
- Stabilize international security architectures & reign in cyber crime

Accelerating Instability In International Security Systems

- Erosion of the post war international security architectures
  - New channels of conflict beyond 3 dimensional space
  - Digital dimension enables targeting of functional dependencies in military systems and socio-economic systems
  - Cyber empowerment of aspiring world powers and many new actors
    - *Scale* due to low barriers to entry, wide availability of hacking skills, readily usable techniques
    - *Proximity* to reach targets globally with short detection times
    - *Precision* in effects and extensibility to target socio-cyber-economic systems
  - Vast attack surfaces are impractical to defend comprehensively
  - Poor awareness of cyber-social conflict and intellectual capacity for defense
- Consequences of erosion
  - Conflict among major actors is less effectively contained
  - Lower predictability in security environment underpinning globalization
  - **Increasing reliance on cross-domain/sector deterrence in an unstable environment of offense-dominance and pre-emption**
    - **Risk of escalation and miscalculation are increasing**
- Growing strategic technical competition among states
  - Advance national champions in strategic sectors (e.g., telecom)
  - Influence on supply chain and standards
  - Changes in the international distribution of economic, technical and military power through large-scale industrial espionage
  - Challenge OECD economies and the liberal international trading system through neo-mercantilism augmented by cyber

Cyber Strategy

Challenge

National and economic security demands robust policy to address:

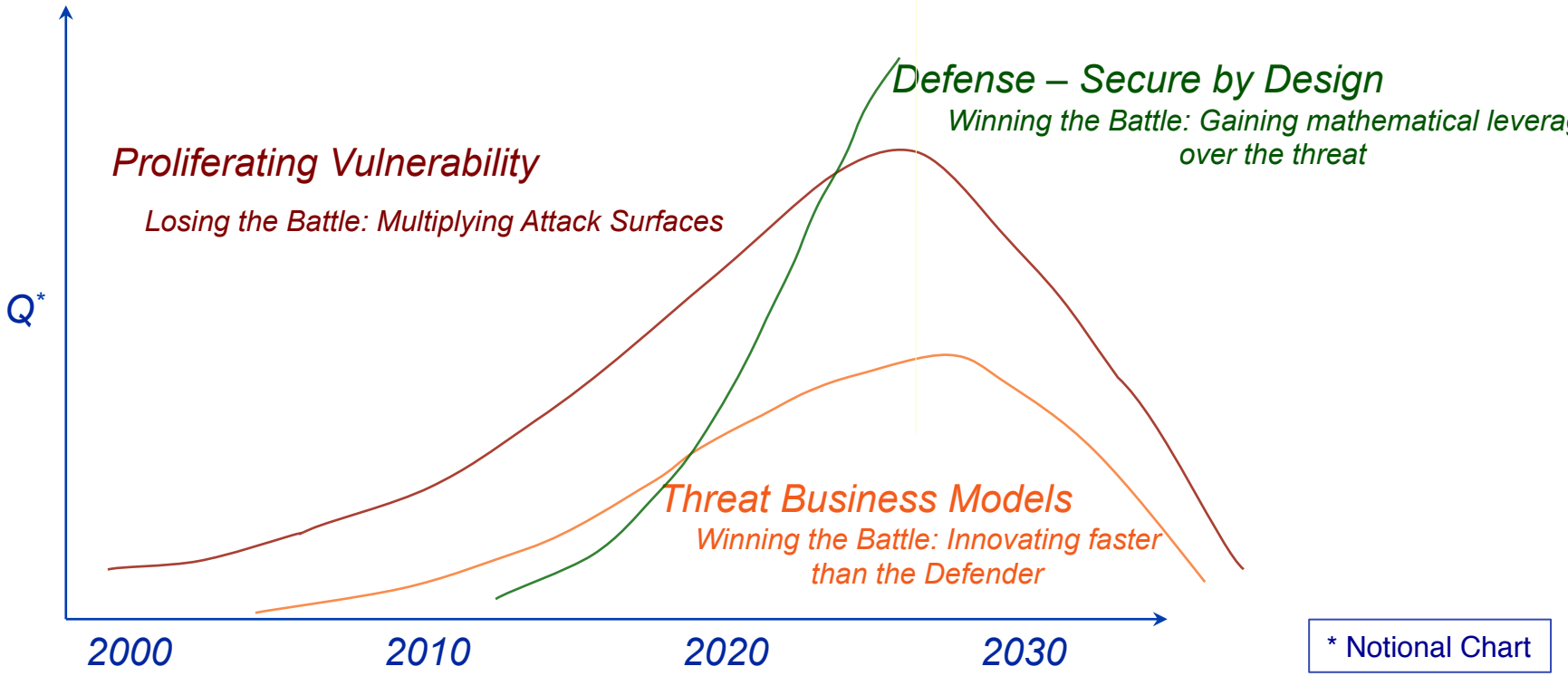
- Proliferating technical and societal vulnerability
- Erosion of international security architectures
- Failing cyber deterrence below LOAC thresholds
- Incentivization of critical actors to overcome public goods dilemmas

Approach

1. **Pursue cyber arms control via global system hardening:**
   - **Raise assurance broadly to constrain offense**
   - Reduce number of destabilizing actors with higher barriers to entry
2. Create measurement frameworks for work factors to support:
   - Leverage,
   - Prioritization
   - Certification & accreditation at system and enterprise levels
3. Raise costs to attackers via defensive coordination
   - Prevent replay attacks to reduce ROI on attackware
   - Instrument attacks better, e.g., via 'kill chain' and 'moving target' architectures
4. Establish international cyber norms to:
   - Enable reputational constraints on state behavior
   - Proscribe and deter critical infrastructure attack
   - Establish deterrence frameworks for malicious behavior below LOAC thresholds
5. Implement industrial policies to:
   - Enable effective ICT markets for information assurance
   - Reallocate cyber risk to actors capable of meaningful technical responses
   - Incentivize critical actors to overcome public goods dilemmas

Effective Cyber Defense: Faster Exponential for Net Defensive Work Factor

Risk = Threat x Vulnerability x Consequences



Non-convergent Risk = (Defense – Threat) x Consequences

Cyber Arms Control: Make Offensive Techniques Obsolete

- *Problem:* Self-restraint is asymmetric
  - Capabilities are opaque
  - Inspection and verification is unlikely
  - Law following states are penalized
  - Cyber offense is eroding traditional strategic stability
- *Solution:* Raising the assurance level, *ergo* better defenses
  - Arms control = foregoing offensive capabilities
  - Cyber arms control = Shift the balance in favor of defense
- Net Deterrence Impact:
  - Reduction in deterrence based on offensive response
  - Must be more than offset by defensive gains
  - Trade deterrence by threatened response for deterrence by denial
- Approach:
  - Enhance resilience of military and civilian systems
    - ❖ Resilience = hardening & survivability
  - Deploy hardened ICT
  - Raise supply chain integrity

Implementation: Raise Assurance To Stabilize State Technical Competition And To Constrain Malicious Activity

- **High assurance host platform** – open source to drive adoption
  - Collaborative international research
  - Best practices for education and industry
  - Integration across technical areas
- **Extend to networking & telecom equipment**
  - Trusted backbones
  - Trusted telephony infrastructures
  - Verifiable equipment
- Encryption
  - Global standards for strength and use
  - Enhanced usability
  - Pervasive encryption in transit and at rest with cryptographically enforced access by state authorities
    - Revocable encryption under cryptographically assured legal standards
- Identity management
  - International digital identities
  - Authentication standards
  - Legal status
- Cyber borders
  - Cryptographic tagging data provenance at the national peering level
    - IPv6 packet staining draft RFC
  - Top down accountability – irrefutable national origination

Verifiable System Programming Language (VSPL)

- Problem
  - Develop an expressive dynamic language designed to support parallelism, verification, and suitable for system programming
- Approach
  - Provide clean language semantics by building from Lambda Calculus precursor languages
  - Enable abstraction-oriented programming, modularity, code reuse
  - Rationalize for parallelism, information control flow, formal verification
  - Architect for type safety, code synthesis, and composable security
  - Develop a verifiable compiler, leveraging prior research (Leroy, 2006)
    - Expose invariants to speed convergence by theorem provers
  - Program at the level of domain to simplify verification and adaptation
  - Design for code reuse, verification by construction, and collaborative software development
  - Design for dynamic security evaluation and introspective monitoring
- Impact
  - Safe languages for programming high-assurance operating systems
  - Verification of compiler, core OS mechanisms and applications
  - High-productivity and agility

VSPL - continued

- Compilation
  - Compiler transforms for efficiency
    - Retain source abstraction
  - ISA independence for retargetability
  - Parallel execution model(s)
    - Leverage modern integrated circuit capacity
- Other issues
  - Rationalize to simplify automatic code synthesis
  - Modular system, component, and functional design to support code reuse, collarboation and evolution
- Metrics
  - Programmer productivity
  - Code reuse rate
  - Software bug rates
  - Software agility

Host Operating Systems

- Problem
  - Deploy several high assurance operating systems capturing the principle alternative OS design approaches
  - Design HW & ISAs to support OSes
  - Design trustworthy hypervisor
- Approach
  - Implement best science & engineering from scientific literature
  - Architect for strong isolation, least privilege, minimal complexity
  - Control (and monitor) information flows
  - Defend cryptographic keys against leakage
  - Design for dynamic verification and ease of certification
  - Provide common operating environment to enable application portability across OS platforms
  - Architect for modularity to enable realistic embedding of new research components
- Impact
  - Speed adoption of best IA science & engineering
  - Eliminate low difficulty attack vectors on host
  - Enable supply-chain security by reducing vectors for Trojan injection

Persistent Transactional Memory (PTM)

- Problem
  - Develop high-assurance high-availability persistent storage
  - Provide fine-grained integrity & confidentiality
- Approach
  - Build atop persistent, transactional virtual memory
  - Build-in ubiquitous versioning and rollback capabilities
  - Support wide range of storage models:
    - File: sequences of bytes
    - Relational
    - Object
    - Graph
  - Incorporate network awareness:
    - Distribution model with location-independent API
    - Support fragment-aware network identifiers
    - Facilities for replication, full reconstitution with n of m DBs, and high-assurance backup
  - Provide non-by-passable access auditing mechanisms
- Impact
  - High-assurance, high-availability host storage
  - Support resilient, replicated network-level storage
  - Enable high-integrity distributed applications
  - Enable rollback to know states in case of compromise

Intelligent Development Environment (IDE)

- Problem
  - Make high-assurance software development easy & agile
  - Deliver ultra-high productivity, massive code reuse, high automation, collaborative integration, and a scalable cognitive footprint
- Approach
  - Develop intelligent algorithms for reasoning about entire computing and application stack
    - Minimum feature/vulnerability software stacks for applications
    - Fast implement-debug-test-verify cycle
    - Resilient programming for mission assurance
  - Exploit unified graph representations for source code, compiler transformations, binary instructions, dynamic changes of representation, migration of storage, semantic annotations of source code
  - Generate & parse graphs to personalized human-friendly formats, including textual source code, data flow visualizations
  - Representations also carry upward to application-specific domains, information flows
  - Integrate design rationales and documentation and utilize natural language I/O for documentation
  - Provide a gentle learning slope and intelligent personal tutoring
  - Maintain positive models of behavior for runtime monitoring and rapid response to deviation from expectations
  - Semantic operations on source code enable dynamic modification of running code based on runtime feedback, introspective programming and self-adaptive programs
- Impact
  - Highly agile development for secure software
  - Dramatically reduced software costs
  - Rapid detection of and response to behavioral deviations

Phased Platform Scaling

- Embedded systems
  - SCADA
  - Cyber physical systems
  - Internet of things
- Cloud hypervisors, emulated OSes
- Windowed systems
  - Mobile: smart phones and tablets
  - Personal computers and work stations

Accelerate IA Education & Research

- Enable hands on experience with state of the science systems
  - Self-documenting development environment
  - Gradual customized learning curve (cognitive footprint)
- Enable frontier research via incremental extension
- Modular platform for testing new components
- Highly effective code reuse, sharing, and collaboration
- Broad availability

Need For International Collaboration

- Science & engineering
  - Leverage complementary expertise
  - Achieve higher total funding
  - Speed development and adoption
  - Benefit from diverse perspectives
  - Educate and train more computer security professionals
  - Build capacity internationally
- Policy
  - Create momentum for higher assurance open source
  - Catalyze defensive virtuous cycles
  - Spread tools to resist malicious cyber actors
  - Incentivize private sector to adopt superior IA architectures

Summary

- Cyber insecurity crisis is deepening
  - Pol-mil interaction with cyber
  - Offense as defense is highly unstable
- Cyber arms control = raising assurance of COTs host
  - Wide adoption necessary for stabilizing impact
- Reference secure host research platforms enable:
  - Accelerated IA research and education
  - Increased trustworthiness of open source supply chain
  - Improved minimum IA best practices for commercial sector
  - Elimination of lower end attack vectors
- Propose funding by research agencies for shared host platforms that include:
  - Verifiable system program language
  - High assurance operating systems & HW ISAs
  - Persistent transactional memory
  - Intelligent development environments
- Incentivize industry
  - Technology inject to open source world
  - Flood markets with high assurance host stack
  - Lower investment risk to best current engineering
  - Raise level of commercial host security
- Stabilize international security architectures & reign in cyber crime