

Summary

The full environment in which business live and work today is fraught with risk elements not directly controllable by the corporate entity. Facing hard reality, both our public and private enterprises cannot ignore the threat of unexpected intrusion resulting in both isolated & large-scale destruction of infrastructure services. Sometimes disruptions are direct, internal and localized; yet also today, disruptions occur because of large-scale slowdowns or failure of critical public infrastructure. Still, most failures result from accidents or oversights. FineGrain Networks builds systems that instantaneously recover from all kinds of failure situations: from a simple server fault to a natural disaster. *Regenerative Service Grid (RSG)* applications systems are secure and self-healing, recovering from partial or system-wide failures in software modules, server platforms and network connections. We use both time-tested and novel structural approaches to ensure that software is secure from intrusion. And because critical applications must adapt quickly to changing needs, we also provide enormous scalability, business flexibility, and on-the-fly problem-solving capabilities.

This is not a simple access-control and firewall based band-aid, it is a comprehensive and collaborative response from a realistic assessment of accidental failures and deliberate mischief.

Security Model

FineGrain Networks takes comprehensive steps to ensure the security of application grids built with its technology:

- Inter-server communications occur over private or encrypted VPNs
- Servers are remote manageable, small, field replaceable units
- Using policy-enabled switches, applications are able to provision their own QoS requirements and security pathways
- Operating systems are DISA certified: Secure Linux or Secure Solaris
- Local access is not permitted to the OS - remote management is coordinated with factory-installed multi-path, Kerberos agents
- Applications run in secure sandboxes - virtual machines isolate applications from OS control
- Honey pots are dynamically deployed to excess capacity servers and automatically trigger domain-based security responses on identification of intrusion
- Upon intrusion detection, affected area servers and domains are automatically turned into playpens, while real applications automatically relocate to healthy resources, self assemble and continue processing
- Binary code is not stored on processing servers; instead it is remotely loaded at runtime from secure code-servers – stealing a server does not give access to application code
- Applications are self assembling from Microservices running on many separated machines – no server ever has a full picture of what is happening
- Security and policy domains are built-in with brokered inter-domain communication controlled by security-policy gateways
- Applications have the ability to move from server to server in the grid, so no server specifically can be identified as a location for an subject specific application-targeted attack
- Inter-process communication is learned by Microservices and not pre-programmed in – this allows adaptation and evolution of not just keys, but communication protocols
- Grid agent technology allows event-driven swarming of counter-intrusion agents throughout the network grid
- The service grid is self-managing and self-healing – when problems occur, it automatically assembles the correct reaction team with full data and tools to respond

Examples of Security Application uses

- Critical corporate infrastructure (RSG-native systems; heritage IT software and hardware; transport systems; communication networks; power, water and fuel feeds; shipping) is managed and secured by deployment of RSG based management applications systems that respond automatically.
- Document and application security provided via deployment across a distributed server and data storage grid, with the linking of policy rules on data treatment and response. Data policy optionally can adapt to immediate environmental conditions such as: the requester, supplier, and the current environmental and security alert states.
- Sensors, process-triggers, data-trawlers, and location-based identification services optionally can invoke local and remote processes. This includes real-time assembly of data from multiple data-stores and sensors and then invocation of customized responses. Specific process deployment occurs in real-time to tailor the response.
- Adaptive encryption, security protocols, and processes – applications load and use whatever is appropriate to the situation. Processes optionally can automatically react to alter themselves to support the internal alert level or external (homeland security alert color) situation.
- Survivability of business service applications during blackouts, isolations, and other disruptions. For example:
 - If a data center loses power, remote areas sense this and applications are automatically relocated elsewhere in the grid network and continue processing. This usually happens in a few seconds.
 - If a data center is isolated via large-scale WAN failure, remote services reload locally from local code-servers, log all actions and later re-synchronize with enterprise applications.
- RSG supports distributed decision making in stressful or emergency situations. RSG supports automatic deployment of policy based procedures and trained individuals during stressful situations requiring immediate and accurate response.
 - Team members have network-based agent avatars that represent them virtually. These avatars will self-assemble teams and coordinate a team's communication. Teams have team-avatars that link to form larger control teams.
 - Fast-reaction teams are assembled in moments by picking the correctly skilled members from the pool in active contact with the network (via terminals, cell phones, wireless PDAs, etc.). Members are selected (for example: by role, skill-level, availability, proximity, and associations with the problem area and customers/suppliers affected) to ensure the full skill mix and experience required. These are invited to join a secure group workspace.
 - Everyone intercommunicates via this workspace and access accumulated data. Processes are invoked automatically by events and adapt as circumstances change.
 - Automatic interface protocols are deployed to connect with, appraise of, and coordinate with, local and national government agencies, financial regulatory agencies, and the press. Similarly interfaces optionally are established and managed with customers, suppliers, corporate partners, and international corporate offices.