cl

Skaion Corporation Capabilities Statement

- **Address:** 51 Middlesex Street, Suite 114 North Chelmsford, MA 01863
- **Website:** www.skaion.com
- **Email:** info@skaion.com
- **Contact:** Terry Champion Robert Durst
- **Phone:** (978) 251-3963
- **Fax:** (978) 418-9175

Core Competencies

Provide quality test support, including test design, setup, execution, metrics and scoring. Help the customer conduct meaningful and realistic computer- or network-related tests to identify the limits of effectiveness of a system under test. Develop new technologies (e.g. kernel introspection) to support the test scenario, or new adversarial models to stress the system under test.

Tools

- User simulation capable of driving desktop applications and getting graphical feedback
  - Activity can be scripted or autonomous
  - Easily extensible through Python scripting
- Introspection to directly read a target host's kernel data structures
- Simulation of large-scale networks with small numbers of traffic-generating hosts
  - Trunk-level traffic generation up to 100 Gb/s
  - Live and stateful: interacts with real servers
  - Individual sessions reflect user preferences
  - Traffic is repeatable without being repetitive, allowing unbounded operation

R&D and Test Support

- Realistic operational environment implementing desktop user activity without host artifacts
- White Team support: test range design, range control, data harvesting and analysis
  - Custom-developed instrumentation probes
- Red Team support
  - Development of custom vulnerabilities and exploits against actual systems
  - Development of modeled attacks for use in emulations, including
    - worms
    - infrastructure attacks
    - email phishing
    - scans and probes

Performance

National Cyber Range (DARPA)

- Phase 1 design support to APL, Sparta, SAIC
- Phase 2 design and implementation of traffic generation for APL
- Phase 2B traffic implementation for Lockheed Martin

Scalable Network Monitoring (DARPA)

- Subcontractor to APL
- Phase 1: infrastructure design, 1Gb/s traffic and attack generation
- Phase 2: infrastructure design, 100Gb/s traffic and attack generation

Dynamic Quarantine of Worms (DARPA)

- Phase 1: developed worms, implemented background traffic generation
- Phase 2: developed custom worms
- Phase 2B: full-spectrum support: traffic generation, testbed control, data analysis, custom worm development, range instrumentation

P2INGS (DARPA)

- DTO's "Reference Data Set Generation" effort: implemented attack scenarios against model distributed network to create data sets for performers to analyze
- Data sets are available through PREDICT

Others

- APL project: realistic host-level user activity, kernel instrumentation and data gathering
- DARPA's MILNET: background traffic generation realistically modeling Joint Service network activity
- AFRL's Advanced Intrusion Detection Test Environment: custom tests to explore the limits of coverage of network intrusion detection systems
- STRATCOM/J8: background network traffic and Internet simulation for Joint Service red-vs-blue exercise (performed under subcontract to Northrop Grumman)
- DARPA's SAPIENT: test design, control and data analysis (performed under subcontract to MIT Lincoln Laboratory)

Recognition

- 2007: DARPA/STO recognition for Sustained Excellence by a Performer—with this we were DARPA/STO's nomination for this recognition across all of DARPA, which was decided at DARPATech 2007. This award was for our performance on Dynamic Quarantine of Worms, where, in addition to our traffic generation, data gathering and data analysis contributions, we developed 10 novel worms in under a year for testing the DARPA performer's solution.
- 2011: IARPA Test & Evaluation Team of the Year award, recognizing prime contractor APL and its subcontractors. In announcing the award, IARPA Director Dr. Lisa Porter cited the team's "quick reaction on evolving instrumentation and infrastructure requirements," which were key Skaion contributions.

Differentiators

- We continue to provide unparalleled capabilities in efficient traffic generation for cyber testing. Our products beat commercial TGSs in terms of cost, realism, non-repetition and support, and compare very favorably in terms of traffic volume and network simulation scope. Customization to the particulars of the test is always encouraged.
- We developed the ConsoleUser, a programmable "brain" that reflects the preferences of a user, to drive desktop applications such as MS Office, Internet Explorer, Acrobat, Windows, Media Player and others as a human would: with keyboard and mouse actions, and with as few detectable artificialities as possible.
  - The ConsoleUser relies on recognizing GUI elements, so support for new applications or even new platforms can be as easy as indexing new images to match and coding new application event logic.
  - The ConsoleUser works transparently with physical hosts or virtual machines using the VNC protocol. (For this reason, interaction with physical hosts requires that they run a VNC server.) Known compatible VM engines include QEMU/KVM, Xen and VMware ESXi.
- We drive user-level network applications instead of generating traffic directly. By playing the part of the users, the applications and host operating system produce network traffic that is guaranteed to be realistic and correct at all layers of the OSI network model.
  - The resulting traffic is live and stateful (traffic generators can interact with real servers) and is indicative of users with preferences and habits.
- We provide rapid extensibility and customization. Because we don't have to reverse-engineer any applications we can quickly support new applications or extensions to existing applications, even if we have never seen them.

Company Data

- Incorporated May 1998
- Veteran-owned Small Business
- Employees are all US Citizens
- DUNS: 032714565
- CAGE Code: 1U1R8
- NAICS: 541712, 541511, 541512, 541519