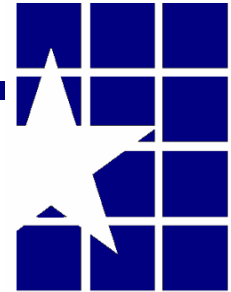


---

# ATC-NY

Architecture Technology Corporation

---



## Empirical Privilege Profiling in an Application Community

Carla Marceau

ATC-NY

Cornell Business and Technology Park

33 Thornwood, Suite 500

Ithaca, NY 14850

(607) 257-1975    (800) 672-1982

# ATC-NY

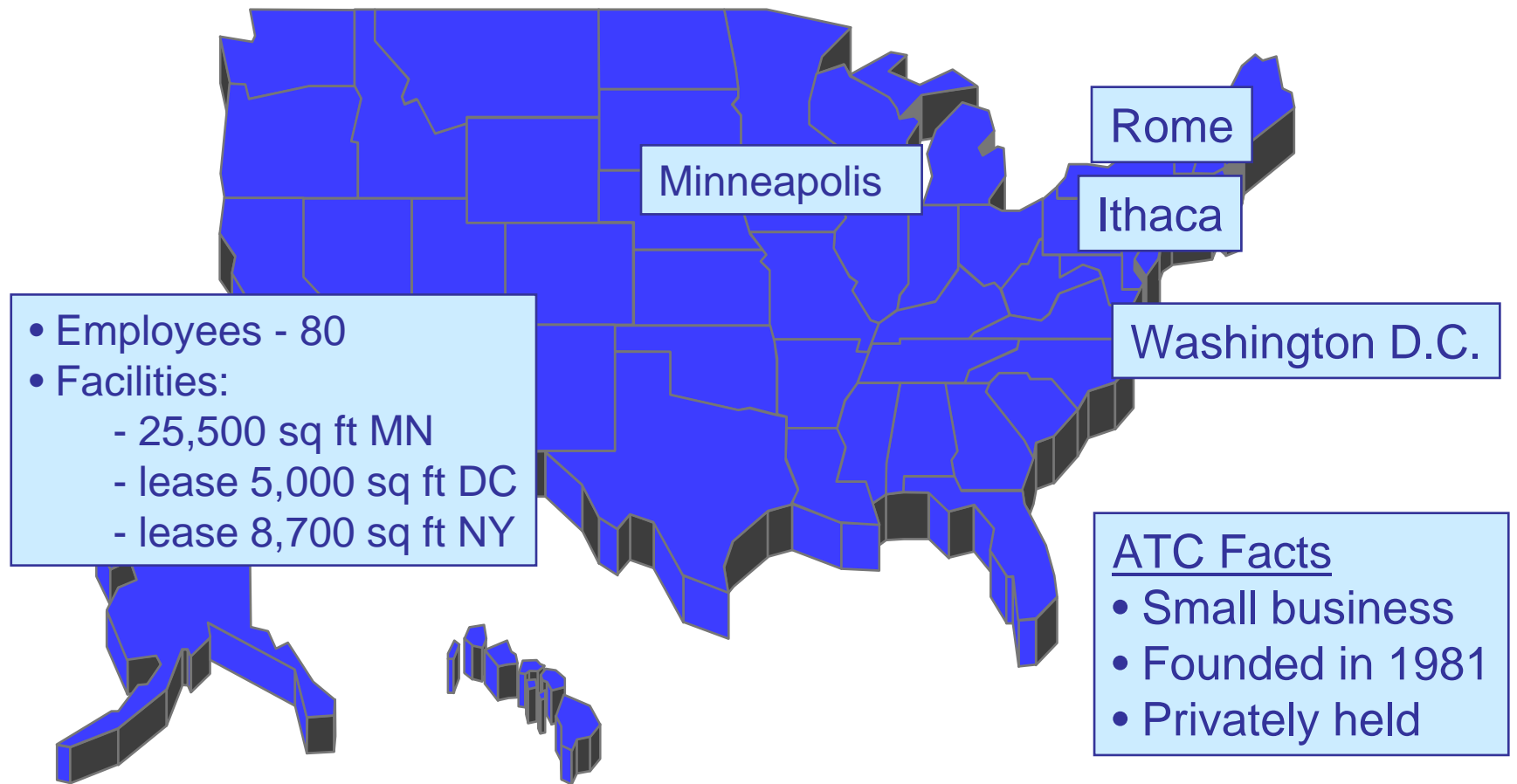
---

- A wholly-owned subsidiary of Architecture Technology Corporation (ATC)
- ATC specializes in distributed computing and network technologies
  - Research and development
  - Engineering services and consulting
  - Network monitoring products: Triticom subsidiary
- ATC-NY
  - 20+ years of experience in advanced R&D and products
  - Specializing in information security, information management, and reliable computing
  - Strong history of collaboration with universities and companies, including Cornell, Dartmouth, General Dynamics, Boeing, Lockheed Martin, and others



# ATC operations

---



# Applicable ATC-NY capabilities

---

- Security research and development, including
  - Anomaly-based intrusion detection
  - Profiling techniques
  - “Neighborhood watch” attack monitors
- Peer-to-peer applications
- Empirical privilege profiling

# Empirical privilege profiling

---

- Concept: Characterize the privileges a program needs in order to run
  - Find out what resources it actually uses and how it uses them
  - Treat program as a “black box” (no source code)
  - Abstract away from particulars of individual hosts and users
- Empirical profiling fits in well with Application Communities
  - Communities can build profiles quickly through collaboration
  - Community members can all share the resulting profiles



# Potential uses for privilege profiles

---

- Implement the Principle of Least Privilege
  - Privileged program installation: Find out what access control rights a privileged program really needs
  - Program development: Find out if the program is exercising more privilege than you intend
- Detect intrusions
  - Anomalous use of privilege
- Detect insider misuse
- Ensure mobile code safety
  - User of code can check that it stays within profile



# Empirical privilege profiling at ATC-NY

---

- ATC-NY has developed an approach to building abstract privilege profiles based on data collected at collaborating hosts
- We have built automatic correlation software to implement the approach
- We have validated the approach with an experiment
  - Created a small Application Community to collect resource use data for a small application
  - Correlated data collected at multiple hosts and produced a privilege profile for the application
  - Shown that the profile is at an appropriate level of abstraction
- A paper on this work will be presented at the New Security Paradigms Workshop next month

# Building and using program privilege profiles in Application Communities

---

Profiles of the resource needs of applications can contribute valuable input to security tools for Application Communities

Correlation techniques developed at ATC-NY automatically create widely applicable profiles that are independent of user-, host-, or site-specific information

Application Communities are ideally suited to both build and use such profiles