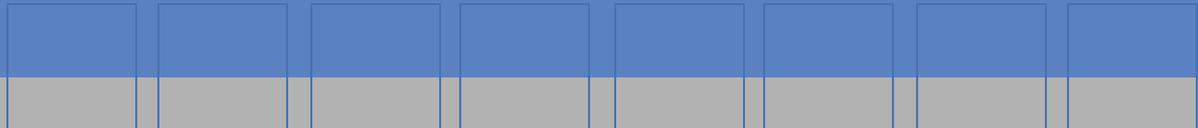


Process Control Systems Forum 2005 Spring Meeting

Research Interest Group

18 May 2005

Dr. Ann Miller
University of Missouri – Rolla



Yesterday's Environment



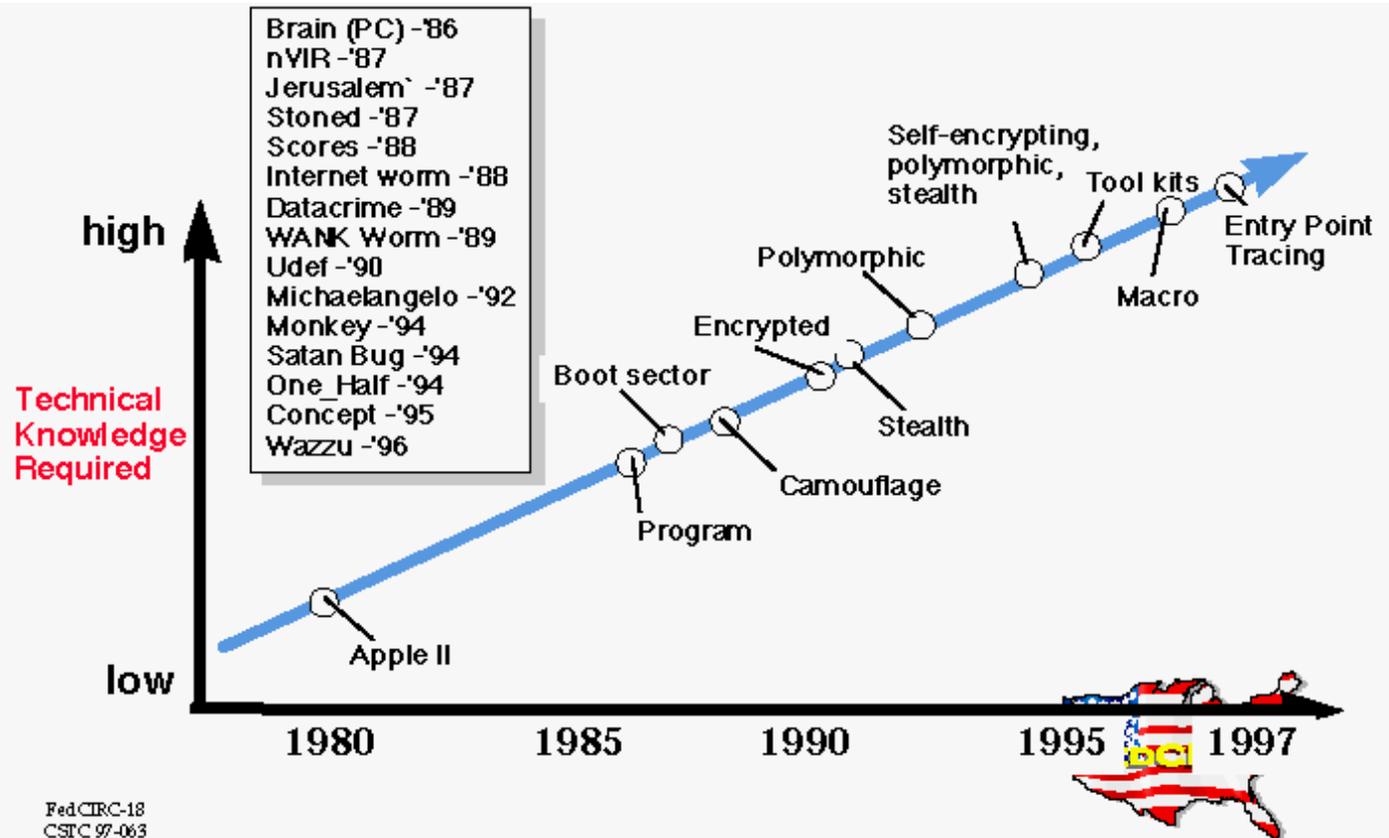
- **Control systems critical**
- **Proprietary protocols**
- **Stand-alone control networks with minimal links to remainder of organization**

Today's Environment



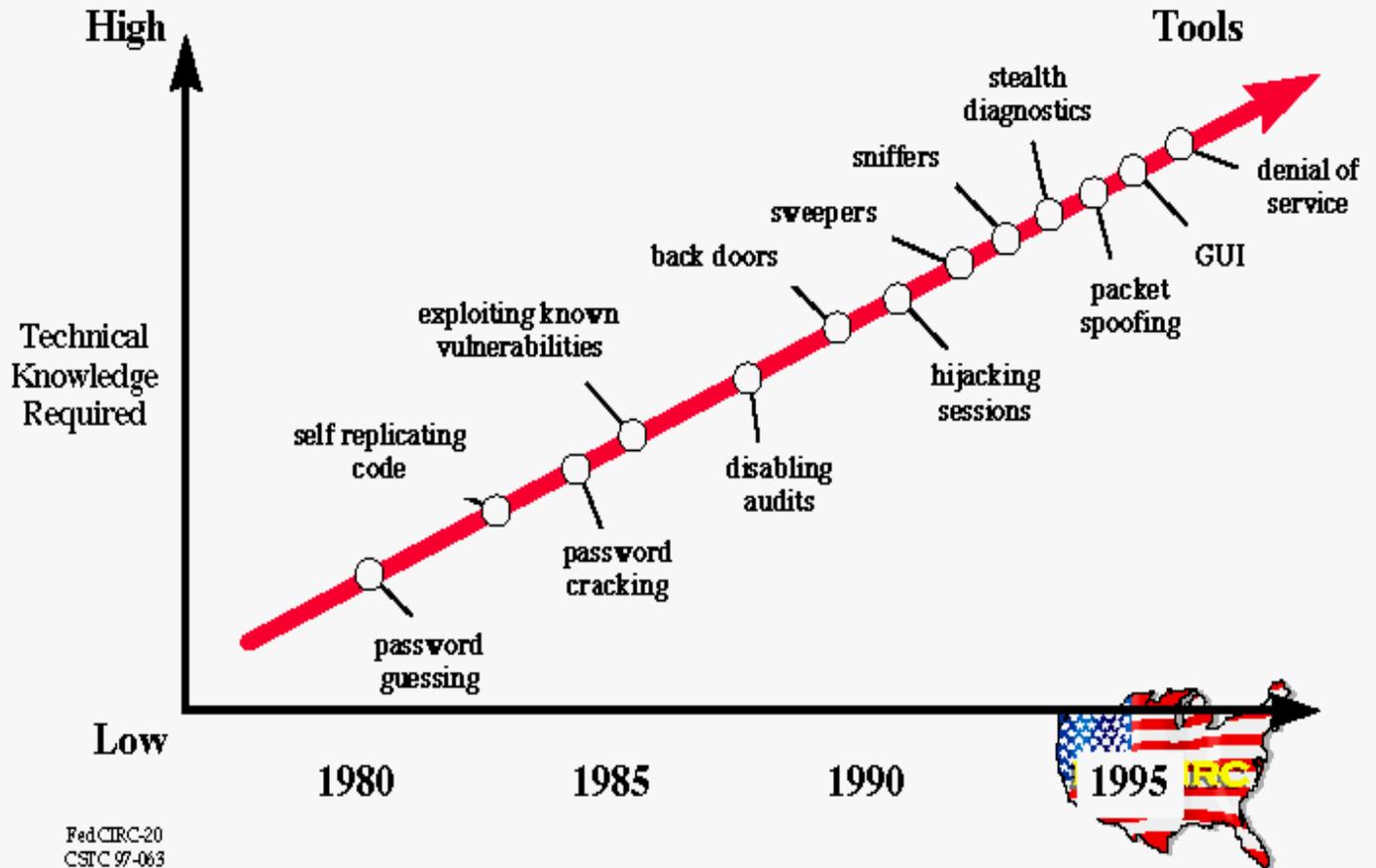
- **Control systems still critical, yet more vulnerable**
 - Ethernet protocol and other standards
 - Increasing use of COTS products with their inherent vulnerabilities, i.e. “one attack fits all”
 - Control systems increasingly networked to the enterprise
- **Number, speed, and sophistication of computer network attacks increasing dramatically**

Sophistication of Attack Programs Increasing



Source - FEDCIRC 1997

Types of Attack Tools Expanding



FedCIRC-20
CSTC 97-063

Source - FEDCIRC 1997

Speed of Attacks Increasing



- **Summer 2001:**
CodeRed infects
360,000 systems in 14
hours
- **Winter 2003: SQL**
Slammer aka
Sapphire infects
100,000 systems in 10
minutes

Tomorrow's Environment



- **Control systems still critical**
- **Control systems even more connected**
 - Network-centric systems
 - System of systems
- **Potential of organized attack, not just the individual “hacker” or disgruntled employee**
 - Organized crime
 - Terrorist group
 - Rogue state

Process Control Systems Forum



■ **Mission**

- Create a cross-industry, cross-functional forum that provides the opportunity for technical exchange with a focus on common needs, consensus architectures, and practices to accelerate the implementation of more secure control systems.

■ **Goals**

- Create an open, collaborative, voluntary forum that leverages the experience and capabilities of stakeholders in the development and adoption of common architectures, protocols, and practices for next generation control systems.
- Develop a partnering strategy intended to leverage knowledge currently dispersed among sectors.
- Stimulate cross-functional discussions between Information Technology (IT) and Operations to strengthen communication and resolve issues inherent within their respective disciplines.
- Define, recommend, and promulgate, protocols and architectures across industry sectors.
- Promote interoperability of common core architecture enabling significant improvements in the field through competitive market forces.
- Utilize innovations developed by the forum to guide requirement gathering, testing, retro-fit, development, and deployment strategies.
- Provide vendors access to multiple industry sectors.
- Facilitate industry access to multiple vendors.

Process Control Systems Research IG



- Interest group to address basic and applied research across the full spectrum of control systems security, including reliability, safety, vulnerability and inter-dependency assessments, intrusion detection, fail-safe and recovery mechanisms, and digital forensics.
- <https://www.pcsforum.org/groups/65/>

Process Control Systems Research Issues



- **Some control systems will be “green field”, that is, new development.**
 - What architectural frameworks best support security, reliability, survivability, etc.?
 - What embedded systems/sub-systems can be inserted to improve the “ilities”?
 - Built-in-self-test
 - Intelligent agents

Process Control Systems Research Issues



- **How do we make existing control systems more immune to attack?**
 - Application-specific techniques
 - Generic approaches
 - Wrappers
 - Intrusion detection systems
 - Intelligent agents
 - Host-based
 - Network-based

Process Control Systems Research Issues



- **What pre-attack indications and warnings can be implemented in the short term? In the long term?**
 - Near-real-time detection
 - Real-time detection

Process Control Systems Research Issues



- **What trans-attack methods can be installed in the short term? In the long term?**
 - Isolation techniques
 - Fault tolerance improvements
 - Survivability mechanisms

Process Control Systems Research Issues



- **What post-attack analyses can be developed to identify attacker and determine attack methodology?**
 - Digital forensics
 - Reverse engineering of code

Process Control Systems Research Issues



- **How can we improve security audits and vulnerability assessments of control systems?**
 - Detailed modeling and reachability analysis tools
 - Boundary control based on reachability
 - High assurance techniques

Process Control Systems Research Issues



- **How can technology be applied to non-technology issues?**
 - Automated security policy checking
 - Use profiling
 - Insider threat detection

- **What are key metrics to determine if we are making progress?**
 - Qualitative
 - Quantitative

Process Control Systems Research IG Goals



- **Create an open, collaborative, voluntary forum that leverages the experience and capabilities of stakeholders in the development of next generation control systems and in the resilience of existing systems.**
- **Develop an inter-disciplinary forum to share research ideas, directions, and results.**
- **Stimulate cross-functional discussions between government, industry, and academia.**
- **Transfer technology innovations shared within or developed by the forum.**

Process Control Systems Research IG



- <https://www.pcsforum.org/groups/65/>
 - annmiller@ieee.org
- **Your participation invited and encouraged**
- **Discussion on the Way Forward**