

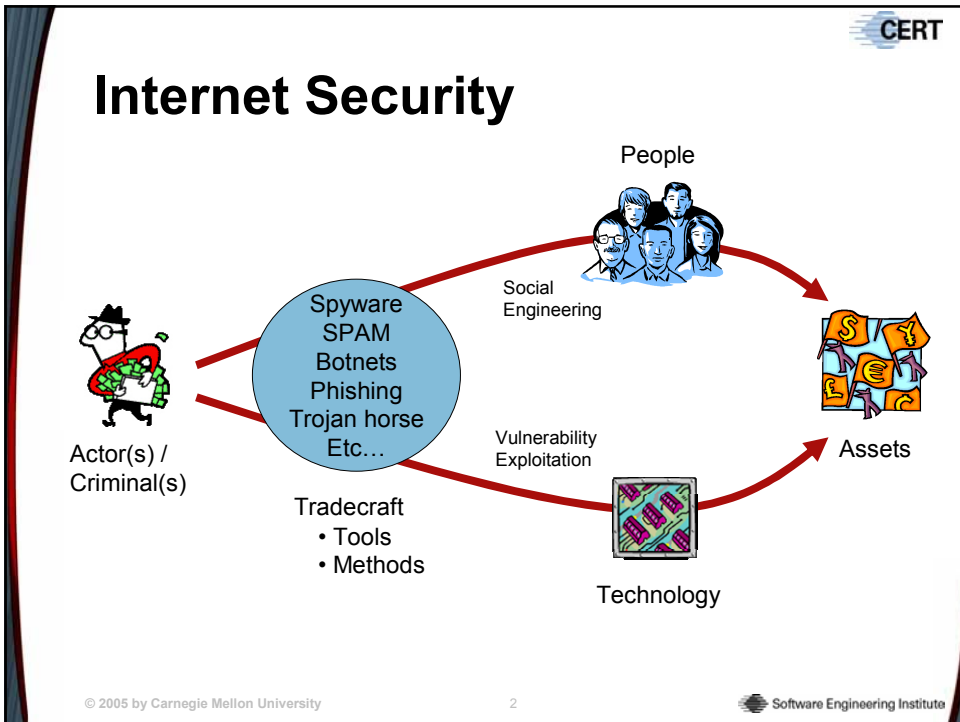
CERT

Artifact Analysis R&D

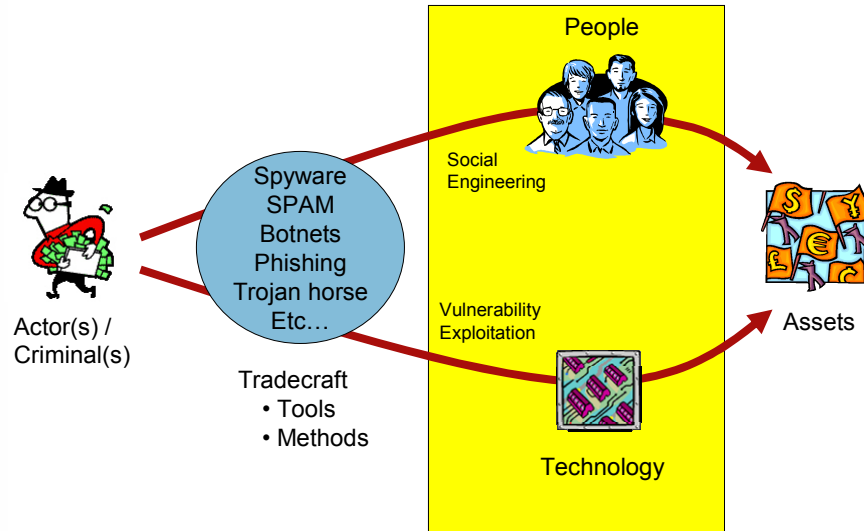
September 5, 2005

© 2005 by Carnegie Mellon University

Software Engineering Institute



Traditional Security Approaches



Technology & People

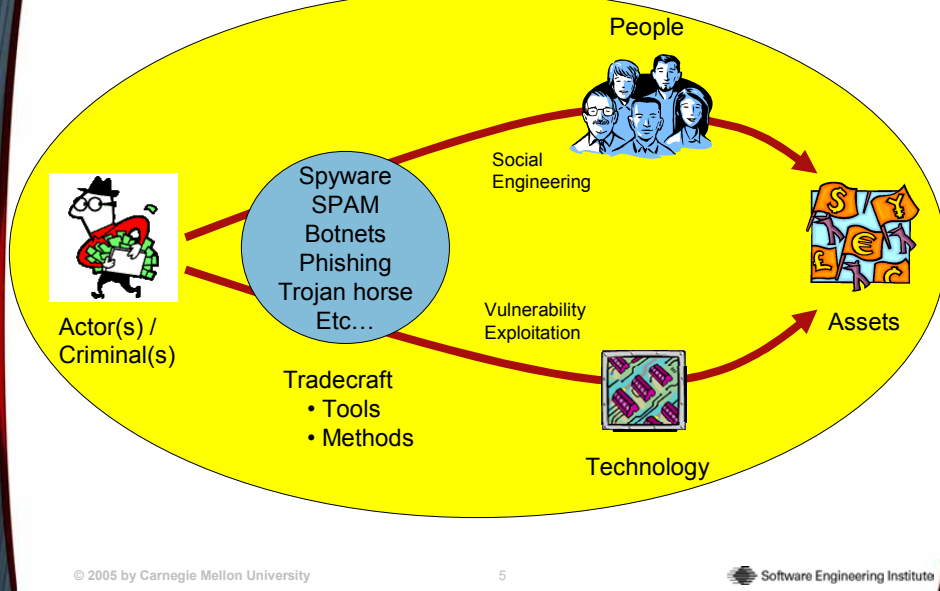
Internet security is a social problem

- People compromise technology
 - Research & improve technology (e.g., people)
- People compromise people
 - Educate & improve people

The common thread is “people compromising...”

- Attribution, law enforcement
- International cooperation

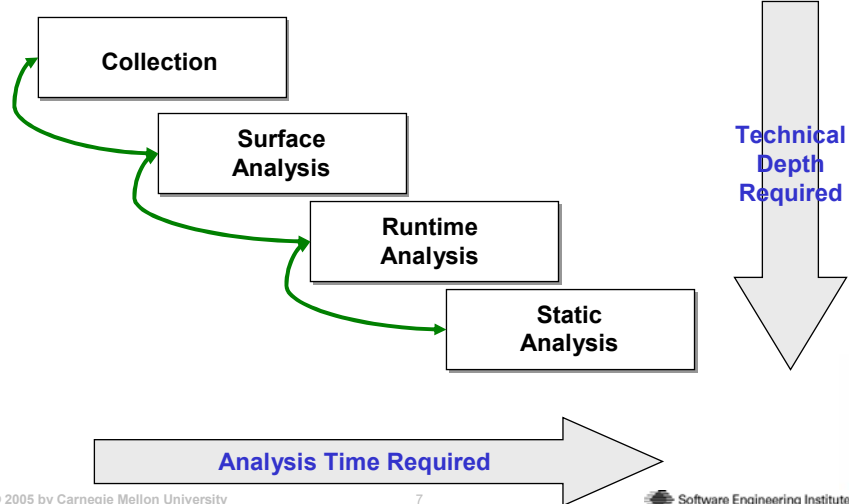
Complete Approach



Roles of Malicious Code Analysis

- Incident response
- Vulnerability analysis
- Attack technology trends
- Threat assessment
- Capability assessment
- Vulnerability assessment
- Law enforcement / forensics
- Signature generation
- Red teaming / Penetration testing
- Attacker competition / crime

Malicious Code Analysis



Malicious Code Analysis

Results:

- Accurate view of attack systems and evolving capabilities
- Accurate insight into targeted assets and resources

Impacts:

- Educate people
- Improve technology
- Pursue attribution

Challenges:

- Immature tools, complex methods
- Lack of formal training / skilled workers
- Information sharing is hard

R&D Goals:

- Reduce analysis time
- Reduce time between attack and legal consequence

What Can Economies Do?

Expand R&D focus beyond attack vector of the day (or worse, yesterday)

- Technology and methodology evolves
 - Malicious / criminal motives remain the same
- Proactive long-term social approach (5-10 years)
 - Incident response = law enforcement
- Approach with R&D investment
 - Decrease value to criminals
 - Increase attribution of and penalties for criminals
 - Decrease time between attack and legal consequence

Short-term Opportunities

- Leverage immaturity of attacker's capability to move assets from cyber to physical world
- Investments in evolving and converging CSIRT technical analysis capabilities with attribution-based (e.g., law enforcement) capabilities
- International cooperation in evolution of effective legal environments that survive changes in technology



CERT[®] Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890
USA

Hotline: +1 412 268 7090

CERT personnel answer 8:00 a.m. —
5:00 p.m. EST(GMT-5) / EDT(GMT-4),
and are on call for emergencies
during other hours.

Fax: +1 412 268 6989

Web: <http://www.cert.org/>

Email: cert@cert.org