



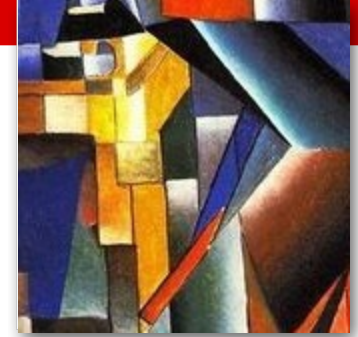
Penetration Testing as an Auditing Tool

March 1, 2011

ISACA Austin Chapter Luncheon

Jeremy Powell, Consultant, atsec information security

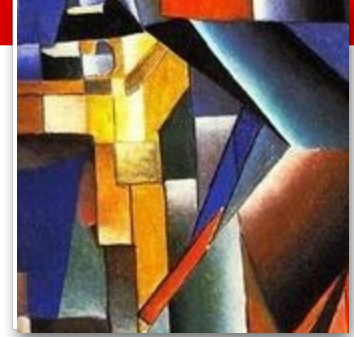
About the Speaker

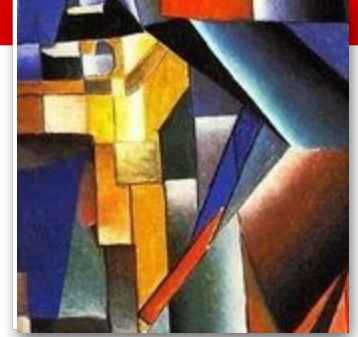


- Security consultant
- Evaluates the security features of:
 - Operating systems
 - Network appliances
 - Cryptographic modules
 - Networks and websites
- Relevant Standards:
 - Common Criteria (ISO/IEC 15408)
 - FIPS 140-2 cryptographic module validation
 - Payment Card Industry Data Security Standard (PCI-DSS)
- Lead penetration tester in atsec U.S. branch

Agenda

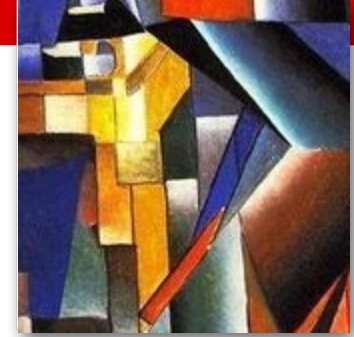
- Assurance and Security
- Breaking the Rules
- Penetration Testing
 - Network and Web Application
 - Physical
 - Social Engineering
- Ethics and Legality
- Complimenting Audits





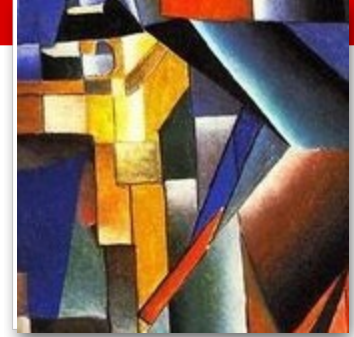
Assurance and Security

- Assurance is established trust in information
- Information might need to be:
 - Accurate
 - Confidential
 - Available
 - Tracked
- How is trust established?
 - Design a sound model
 - Implement the model
 - Regularly audit the implementation against the model
 - Break the model
 - Lather, Rinse, Repeat



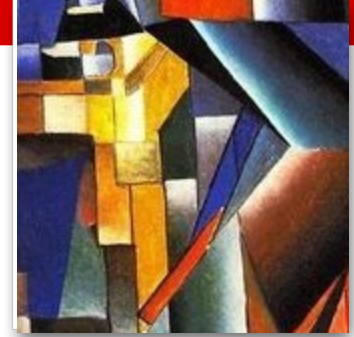
Breaking the Rules

- Models are often based on assumption
- All prison guards are trusted.
 - Bribes
 - Planted guards
 - Impostors
- No one knows how the system is designed
 - Reverse engineering
 - Someone leaks the plans
- No one can have a weapon inside airport security
 - Cleaning supplies inside concourse
 - Restaurant utensils



Penetration Testing

- Controlled rule breaking
- Simulated attack scenarios
- Different Types
 - Network
 - Web application
 - Physical
 - Social engineering
- Different Approaches
 - White box – prior knowledge
 - Black box – no prior knowledge
- Tests assumptions that may have been made that are not true



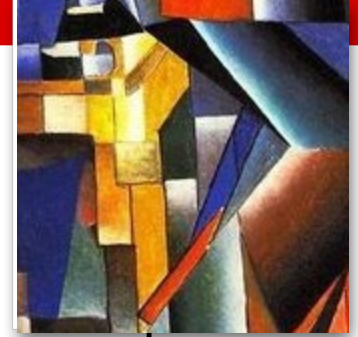
Network and Web Applications

- Goal: Remotely access a host system and:
 - Gain control over the host
 - Read and change sensitive information
 - Use this host to access other hosts
- Techniques
 - Port scanners
 - Vulnerability scanners
 - Exploitation engines
 - Scripting languages
- Common attacks
 - SQL Injections
 - Buffer overflows

Username:
ex: pat@example.com

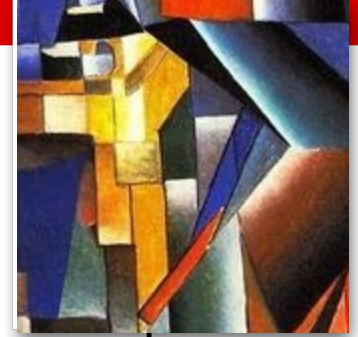
Password:

Stay signed in



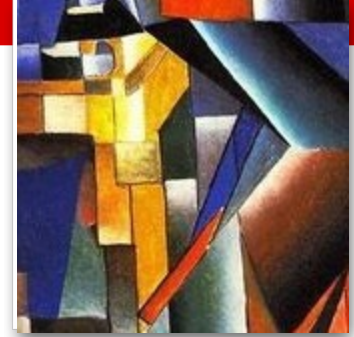
Physical

- Goal: Gain access to restricted areas of a facility (through technical means)
- Tools
 - Lock picks, Screw drivers
 - Laser pointers (for motion sensors)
 - Wireless tools
- Attacks
 - Picking locks
 - Avoiding camera site lines
 - Using key logger to steal passwords
 - Finding alternate entrances
 - Installing rogue access points



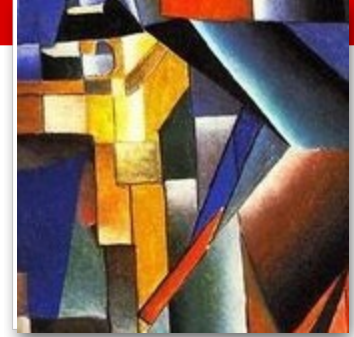
Social Engineering

- Goal: Gain access to restricted areas of a facility (through social means)
- Tools and techniques
 - Non-public but non-secret information
 - Tail-gating through restricted doors
 - Taking advantage of social norms
 - Posing as maintenance workers
 - Acting confident
 - Acting irritated
 - Acting ...



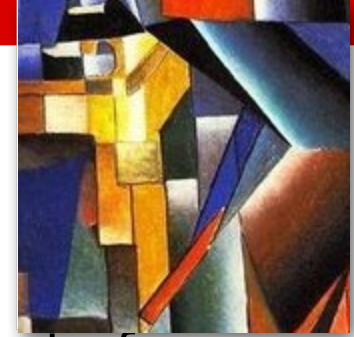
Ethics and Legality

- Testers must be very well trusted
- Contractual Rules of Engagement
 - Defines the exact scope of testing
 - Defines how testers should react if they identify vulnerabilities
 - Constrains the testing to certain limitations
 - In turn, provides tester a “Get Out of Jail Free” card
- Private investigation licenses
 - State of Texas requires testers to be licensed
 - Similar laws around the country
- Disclosure of any discovered vulnerabilities is at the customer's discretion only!



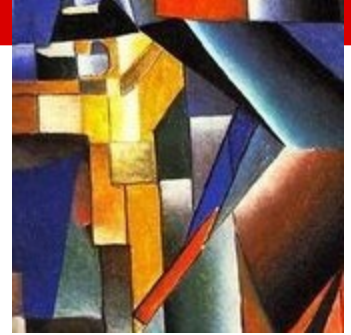
Complimenting Audits

- Auditors may draw incorrect conclusions
 - Audits are based on presented (possibly incomplete or incorrect) evidence
 - Auditors often sample the evidence
 - Auditors may make assumptions
 - The standard or model may be broken
- Penetration testing covers these gaps
 - Testers have simple yet strong motivation
 - Testers may not have seen the audit, therefore they may not have made similar assumptions
 - With competent testers, penetration testing reveals what competent attackers are capable of



Further Information

- The Art of Deception: Controlling the Human Element of Security, Kevin Mitnick, William Simon
- The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers, Kevin Mitnick, William Simon
- atsec's website:
www.atsec.com
- atsec's news blog
<http://atsec-information-security.blogspot.com/>



Thank you.